Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel

Havelange, Benedicte; BURKERT, Herbert; Boulanger, Marie-Helene; Lefebvre, Axel; Poullet, Yves; de Terwangne , Cécile

Publication date:
1996

Document Version
le PDF de l'éditeur

CENTRE DE RECHERCHES
INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES
NOTRE-DAME DE LA PAIX

Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel

Rapport Final

Yves POULLET
Bénédicte HAVELANGE
Axel LEFEBVRE

Avec la collaboration de :
Marie-Hélène BOULANGER
Herbert BURKERT
Cécile DE TERWANGNE

Décembre 1996
Commission Européenne - DG XV
Contrat ETD/95/B5-3000/165

Remerciements

Les auteurs adressent leurs sincères remerciements à tous ceux qui les ont aidés, par leur contribution à la recherche, l'apport d'informations et de commentaires, ou par la relecture du manuscrit, et en particulier:

Les fonctionnaires de la Commission européenne (DG XV),

Les membres des autorités nationales européennes de protection des données,

Les spécialistes de la protection des données personnelles dans différents pays, et spécialement au Canada, Aux Etats-Unis et à Taiwan,

Mesdames Sophie Louveaux et Nancy Risacher,

Monsieur Wolfgang Kilian.

Table des matières

Introduction générale

CONTEXTE DE L'ÉTUDE

A l'approche de l'échéance de 1998, c'est-à-dire de la transposition de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1] dans les législations nationales, le texte européen constitue y compris à l'extérieur de l'Union européenne, un des instruments majeurs de la protection des données à caractère personnel.

Cette directive garantit le respect des libertés et des droits fondamentaux concernant le traitement des données à caractère personnel dans tous les États membres. Afin que cette protection ne soit pas réduite à néant par un simple transfert des données hors du champ géographique de l'application des dispositions européennes, celles-ci prévoient en leur article 25 que le transfert de données à caractère personnel vers un pays tiers ne peut avoir lieu que si le pays tiers en question assure "un niveau de protection adéquat".

Les Etats membres doivent donc examiner les demandes de flux transfrontières pour déterminer si le pays destinataire de ces données assure un niveau de protection adéquat.

---

[1] Ci-après "directive". Pour la suite de ce rapport, on notera que le vocabulaire utilisé est celui de la directive; si un sens différent lui est donné, cela sera précisé.

QUALITÉS DU SYSTÈME

L'étude confiée au Centre de Recherches Informatique et Droit des Facultés Universitaires Notre-Dame de la Paix de Namur vise à offrir à la Commission européenne un outil permettant d'évaluer l'adéquation de la protection accordée aux données à caractère personnel dans le pays tiers à la Communauté.

Cette méthodologie d'évaluation implique que soient rassemblées toutes les informations pertinentes pour réaliser une évaluation de la protection offerte dans le pays tiers, et cela comme le précise la directive, "au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts" donnés.

Dans la mesure où, d'une part, les circonstances entourant le flux ou la catégorie de flux peuvent varier considérablement, et où, d'autre part, la liste des instruments de protection des données peut toujours s'enrichir, l'instrument d'évaluation doit être adaptable à toutes les situations susceptibles de se présenter. C'est un instrument très souple qui permet de traiter la diversité des cas existants.

La méthodologie proposée constituera pour les Etats membres un système d'aide à la décision; il ne s'agit donc aucunement d'un système expert offrant des réponses mathématiques.

QUELQUES ILLUSTRATIONS

Afin d'introduire cette étude, détaillons quelques exemples qui illustrent la diversité des flux transfrontières. Leur brève description nous permettra de pouvoir illustrer tel ou tel point de nos raisonnements tout au long des développements qui suivent.

Le premier exemple est la création par une multinationale américaine disposant de sièges en Europe d'une banque de données relatives au personnel de cadre, où qu'il soit, et recensant des renseignements de tous ordres: ambitions, formation reçue, hobbies,... Il s'agit, pour cette multinationale, de pouvoir répondre facilement à des besoins internes de la compagnie comme celui de la constitution d'équipes de prospection d'un nouveau marché, de la recherche de formateurs, voire de la création d'une équipe sportive,... Ces données collectées à partir de multiples sources -formulaires ou interviews lors des candidatures, appréciation par des supérieurs hiérarchiques, participation à des cycles de formation- sont en l'occurrence assemblées et envoyées à partir de lieux divers (centres de formation, directions du personnel des différentes entités locales,...) aux services centraux de direction du personnel de la multinationale. La banque de données localisée au siège central de la multinationale est accessible par les différents sièges locaux.

La délocalisation d'activités dans des pays du tiers monde suggère un deuxième exemple. Soit une entreprise belge de listes d'adresses travaillant sur les marchés belges et hollandais et décidant de sous-traiter l'ensemble de ses activités d'encodage, de triage, voire de sélection, dans un pays africain. Les données sont collectées principalement auprès de la personne concernée à partir d'un vaste questionnaire portant sur les habitudes de consommation (voyages, alimentation, culture,...). Elles sont croisées avec d'autres données: numéro de téléphone, importance de la localité, type de quartier (revenu moyen par habitant, etc...) provenant de sources publiques accessibles directement de l'étranger ou transférées par support informatique.

Les données sont exceptionnellement transmises directement d'Afrique à un autre pays tiers, où un client de l'entreprise belge désire tester auprès d'un échantillon représentatif contacté par publipostage ou par téléphone l'intérêt pour un produit que cette entreprise étrangère s'apprête à lancer sur le marché belge.

Le troisième exemple est celui de grands systèmes informatisés de réservation aérienne[2]. L'un des plus importants d'entre eux est localisé pour les cinq continents aux Etats-Unis, et gère quotidiennement 2.000.000 de réservations venant du monde entier. Cela signifie que chaque jour, chaque seconde, des données à caractère personnel sont traitées par cette société. Ces données sont enregistrées sous forme de "Passenger Name Record" (ou PNR). Outre le nom et l'adresse des passagers, ces PNR contiennent leurs destinations aériennes, leur état de fumeur ou non, ainsi parfois que les hôtels qu'ils choisissent, les voitures qu'ils louent ou encore leur numéro de carte de crédit.

Le phénomène "Internet" suggère enfin d'autres exemples: on peut citer la présence sur Internet de nombreux fichiers, annuaires téléphoniques, listes avec photos et curriculum vitae de membres d'institutions universitaires, photos de personnes recherchées par la police,... Ces fichiers et listes contiennent des données collectées à partir de tous points du globe et consultables de la même manière.

Il est difficile, on le pressent, d'aborder ces divers flux de la même manière, tant sont différents leurs contextes: les flux à l'intérieur d'une multinationale décrits au premier exemple visent une catégorie bien particulière de personnes -le personnel de la multinationale- et circonscrivent, à première vue du moins, les risques aux seules relations de travail.

Le deuxième exemple vise une catégorie de population plus vaste. Certains flux s'opèrent sur base de supports traditionnels

---

2 Tels les systèmes Galileo ou Amadeus, dont le fonctionnement est détaillé dans: ARETE, *Les réseaux internations et la protection des données personnelles*, Etude pour la commission des communautés européennes (DG XV), Mars 1995.

(papier, par exemple). Les finalités liées à l'utilisation "marketing" des données collectées et intégrées peuvent être poursuivies par des entreprises multiples sises en Europe ou à l'étranger. On note également à propos du second exemple que les opérations matérielles de traitement (hormis la collecte) sont situées hors Europe alors que l'entreprise pour le compte de laquelle le traitement est opérée est située en Europe.

Le troisième exemple se caractérise par le fait qu'une multitude de flux particuliers opérés à chaque fois pour répondre à des demandes individuelles, peut entraîner des possibilités infinies de réutilisation hors Europe.

Enfin, les exemples liés au phénomène Internet appellent la remarque suivante: la mise sur un site d'une information nominative ou d'un message destiné à un forum de discussion ouvert, même si elle a pour l'émetteur une finalité déterminée, permet à cette information ou à ce message d'être utilisés pour de multiples finalités par la variété indéterminée de personnes ayant accès à ces informations. Ainsi, un curriculum vitae mis sur Internet peut être utilisé par des employeurs potentiels, des sociétés de marketing, d'autres chercheurs d'emploi, une administration de sécurité sociale, voire une secte,...

PLAN DE L'ÉTUDE

Cette étude présente tout d'abord un bref descriptif du champ de notre travail (chapitre I). Il s'agit de délimiter et décrire les hypothèses à étudier et analyser les éléments de la Directive y afférant.

Un second chapitre examine la nature des risques existant pour la personne concernée lors d'un transfert de ses données hors de l'Union Européenne. Il s'attache ensuite à déterminer quels facteurs peuvent aggraver ou diminuer ces risques, eu égard à la

nature particulière du flux envisagé. La protection est en effet "adéquate" en fonction de ces risques, et tente de couvrir ceux-ci.

Un troisième chapitre vise à déterminer le contenu de la protection adéquate, dont on verra qu'elle se structure autour de quatre principes de fond. Vient alors l'examen des moyens d'effectivité de cette protection, c'est-à-dire, des éléments qui assurent *in concreto* le respect des principes de fond, en les exprimant, en assurant leur mise en oeuvre et permettant un recours (et éventuellement prévoyant des sanctions) en cas de défaillance.

La dernière étape de ce travail (chapitre IV) consiste à appliquer la réflexion conceptuelle qui précède aux cas qui peuvent se présenter dans la pratique. Nous proposons ainsi un outil d'aide à la décision, pour l'évaluation de la protection du pays destinataire de flux en fonction des caractéristiques (risques, facteurs d'aggravation ou de diminution du risque,...) propres à ce flux. Bien sûr, on veille encore à souligner ici qu'il s'agit bien d'un outil d'aide à la décision et non d'un instrument fournissant des réponses finales. La méthodologie proposée sera enfin "testée" grâce à différents exemples de flux transfrontières inspirés de cas réels.

AVERTISSEMENT

La présente étude a pour objet la présentation d'une méthode d'analyse en vue de déterminer l'adéquation de la protection des données dans les flux transfrontières au sens de l'article 25 § 2 de la directive. Dans le cadre de la réflexion menée, les auteurs ont développé nombre de questions corrélées à cet objet précis:

- premièrement,la question des domaines d'application respectifs de l'article 26, de l'article 4.1 (c) et de l'article 25 et la question de l'application combinée de ces articles;

- deuxièmement, les questions liées aux différents niveaux d'analyse prévus par l'article 25 dans ses différents paragraphes;

- troisièmement, la question du contrat comme technique de protection des données, au sens des articles 25 et 26.

La recherche a également amené les auteurs à analyser de manière plus précise deux systèmes de protections: celui offert par la récente législation taïwanaise, et celui récemment proposé par la Canadian Standard Association.

Ces réflexions complémentaires ou annexes n'ont point été reprises dans la présente étude que les auteurs, à la demande de la Commission européenne, ont strictement limitée à l'objet précis demandé par le cahier des charges. Elles feront l'objet de publications séparées.

Chapitre I. Descriptif du champ de l'étude

L'objet de ce chapitre est d'analyser brièvement le texte de l'article 25.1-2 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette analyse vise à circonscrire précisément le cadre de cette étude, même si son propos n'est pas de faire l'analyse du texte de la directive.

INTRODUCTION

En vertu de l'article 25.1 de la directive, "les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat". Le principe est donc l'interdiction du transfert, sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de "toutes les circonstances relatives à un transfert ou à une catégorie de transferts" et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et certains concernent le niveau de protection en vigueur dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées (ce dernier mot implique

une évaluation de l'effectivité de ces éléments de protection. Nous y reviendrons).

SECTION 1. RÉFLEXIONS PRÉLIMINAIRES

Trois remarques s'imposent d'emblée au sujet de la notion d'"adéquation".

(i) Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question: "par rapport à quoi la protection doit-elle être adéquate"?). Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer, comparer la protection du pays tiers.

(ii) Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut "en particulier" prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

(iii) Enfin, le contenu de ces éléments n'est pas défini: si par exemple on sait qu'il faut prendre en compte la durée des traitements, la directive n'indique pas plus avant ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devraient être le "contenu minimum" d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection.

L'appréciation du caractère adéquat de la protection offerte dans le pays tiers suscite encore deux questions importantes,

examinées dans les deux sections qui suivent. La première porte sur la notion même d'"adéquation" (Section 2); la suivante concerne la marge de manoeuvre dont disposent les Etats membres dans le cadre de l'article 25 (Section 3).

SECTION 2. NOTION D'"ADÉQUATION"

L'article 25 de la directive requiert un niveau de protection "adéquat" dans le pays tiers; l'utilisation du terme même d'"adéquation" a suscité de nombreuses controverses, que ce soit au sujet de l'approche que requiert cette notion (2.A), ou au sujet de la différence des exigences de la directive et de la Convention 108[1] (2.B)

2.A. Approche de la notion de "protection adéquate"

La notion d'adéquation requiert une approche au cas par cas (i), pragmatique (ii) et fonctionnelle (iii). Il ne s'agit certainement pas ici de faire une comparaison abstraite de deux textes: il faut tenir compte à la fois de la réalité du transfert ou de la catégorie de transferts considérés, et de la totalité des éléments qui peuvent assurer dans le pays tiers la protection des données transférées.

(i) Approche au cas par cas

D'après l'article 25.1[2], le caractère adéquat doit être évalué *par rapport à un transfert déterminé ou à une catégorie de transferts.*

---

1 Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981, ci-après dénommée Convention 108.

2 On évoquera plus tard la possibilité de constatation du niveau adéquat plus globale, comme le suggère l'article 25.6.

C'est pourquoi on recommande d'étudier tout d'abord les risques liés à ce flux ou à cette catégorie de transferts, avant de déterminer si le pays tiers offre un niveau de protection adéquat pour ces risques précis. Dès lors, si une protection adéquate n'existe que dans certains domaines restreints (secteur bancaire ou de la santé, par exemple), mais qu'il s'agit précisément des domaines concernés par ce flux, le niveau de protection pourrait être considéré comme suffisant pour autoriser le transfert.

Cela représente une différence fondamentale avec une autre approche possible de la notion d'adéquation, qui serait légistique et abstraite, entièrement fondée sur les textes. L'approche retenue par la directive est résolument pragmatique: c'est concrètement que doit s'apprécier la protection.

(ii) Approche pragmatique

L'article 25.2 de la directive renvoie à une diversité de règles, normes, instruments ou systèmes de protection[3] à prendre en compte: le rôle des instruments législatifs est important (et facilite l'évaluation), mais l'approche retenue veillera à pointer d'autres types de règles pouvant offrir une protection aux données à caractère personnel faisant l'objet du flux, qu'il s'agisse de codes professionnels, de la jurisprudence, de principes du droit, des statuts des entreprises,... Outre ces instruments, une protection adéquate requiert que l'effectivité des règles soit assurée: ici aussi, une série de mécanismes existent et sont pris en compte dans la méthodologie proposée.

---

[3] Il est même envisageable de considérer que certaines mesures techniques, du type des PICS (Protocol for Internet Content Selection), par exemple, puissent être considérées comme système de protection.

(iii) Approche fonctionnelle

L'approche retenue ne vise pas nécessairement à tenter de retrouver dans les pays tiers les mêmes dispositions que celles énoncées par la directive, mais bien à s'assurer que d'une manière ou d'une autre, le pays tiers offre des garanties en matière de protection des données par rapport au flux ou à la catégorie de flux envisagés. L'accent sera mis sur les moyens reflétant les principes fondamentaux de la protection des données . C'est donc à tous points de vue (principes protégés et moyens d'effectivité) une "similarité fonctionnelle"[4] qui est recherchée. La "similarité fonctionnelle" implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si les dits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète.

2.B. Notion de protection équivalente dans la Convention 108

Il est parfois soutenu qu'une protection "adéquate" serait nécessairement moins exigeante qu'une protection "équivalente", telle celle requise par la Convention 108.

La Convention 108 prévoit en son article 12 l'obligation de permettre le flux de données vers un autre État Partie à la Convention si cet État assure une protection équivalente, ce qui fait l'objet d'une présomption. S'il n'existe pas de protection équivalente dans le pays destinataire (parce que, pour une catégorie particulière

---

4 Voir à ce sujet, J. REIDENBERG, Setting Standards for Fair Information Practice in the USA, *Iowa Law Review*, March 1995, Vol. 80/n°3, pp.

de données qu'elle juge plus sensible, une Partie a prévu une réglementation plus exigeante), la Convention prévoit la possibilité de déroger au libre flux transfrontière de données. En ce qui concerne les flux transfrontières vers les pays tiers non signataires, la Convention 108 ne prévoit rien. Le pays émetteur peut aussi bien restreindre ou interdire les flux vers ces pays, que les autoriser purement et simplement.

Le principe de la Convention 108 est donc l'obligation de liberté des flux transfrontières entre États Parties à la Convention dans la mesure où existe une protection équivalente, et la faculté d'y opposer des restrictions dans l'hypothèse inverse ou dans le cas de flux vers les pays non signataires.

Par contre, on l'a vu plus haut, le principe de la directive est d'interdire les transferts vers les pays tiers où n'existe pas un niveau de protection adéquat.

Il faut se garder de conclure que les exigences de la Convention 108 sont plus lourdes que celles de la directive en se basant sur la comparaison entre les termes "équivalence "et "adéquation". En effet, cette comparaison n'est pas pertinente dans la mesure ou ces termes ne visent pas les mêmes hypothèses. La Convention 108 ne règle pas la question des flux vers les pays non signataires, alors que la directive européenne, elle, interdit les flux vers les pays, *tiers* à la Communauté européenne, dès lors qu'ils n'assurent pas une protection adéquate.

SECTION 3. LA "MARGE DE MANOEUVRE" DES ETATS MEMBRES

3.A. Analyse du texte

Un des buts principaux des rédacteurs de la directive était d'obtenir une politique commune des États membres par rapport à la

problématique des flux transfrontières: "(...) la libre circulation des données entre les États membres, que la présente proposition de directive vise à instaurer, suppose que des règles communes soient adoptées en ce qui concerne les transferts vers les pays tiers"[5].

Si le but premier est bien que la Communauté européenne développe une politique commune en la matière, il n'en reste pas moins que l'article 25 suscite une question importante concernant les disparités qui pourraient exister entre les positions des États membres face aux flux transfrontières. Cette question préoccupe de nombreux spécialistes[6] qui se sont penchés sur la rédaction de l'article 25 de la directive, selon lequel "(...) le transfert (...) ne peut avoir lieu que si, *sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive*, le pays tiers en question offre un niveau de protection adéquat". En d'autres termes, on peut se demander de quelle marge de manoeuvre les États membres disposent pour édicter des règles éventuellement plus strictes ou plus complètes que celles de la directive.

Des disparités dans l'appréciation de la légitimité du transfert pourraient donc se présenter en ce qui concerne les flux transfrontières: c'est cette question qui est examinée au point 3.B. ci-dessous.

---

5 Exposé des motifs de la proposition modifiée (deuxième version) de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 30 juillet 1992, p. 35.

6 Voir entre autres: Y. POULLET, "The European Directive relating to the protection of physical persons with regard to the processing of personal data and its free circulation-a state of relative harmony", in *A Business Guide to Changes in European Data Protection Legislation*, Cullen International, Novembre 1996; S. SIMITIS, From the Market to the Polis, The EU Directive on the Protection of Personal Data, *Iowa Law Review*, March 1995, Vol. 80/n°3, pp. 463 et suiv.; P. SCHWARTZ, European Data Protection Law and Restrictions on International Data Flows, *ibidem*, pp. 487 et suiv.

3.B. Légitimité du transfert

Certains États membres pourraient avoir une législation plus exigeante que d'autres sur certains points, par exemple en matière de données sensibles.

Ces exigences pourraient les amener à refuser tout transfert de ces données si certaines conditions ne sont pas remplies (par exemple, accord écrit pour les données médicales), ce qui amènerait des disparités, car d'autres États membres pourraient, eux, accepter le même transfert sans conditions particulières. Ce problème se situant en amont de celui de l'appréciation du niveau de protection offert par les pays tiers, il n'entre pas dans le champ de cette étude.

SECTION 4. REMARQUE FINALE

Certaines dispositions de la directive peuvent être mises en relation avec l'article 25. Ainsi, l'article 26, qui prévoit les dérogations à l'article 25, ou encore l'article 4.1 (c), en matière de droit applicable aux traitements de données à caractère personnel. Quoique l'étendue et les implications de ces articles suscitent des questions importantes, elles ne constituent pas l'objet de cette étude, et ne seront donc pas prises en compte dans le cadre du présent rapport.

Chapitre II. Risques et facteurs d'influence

SECTION 1. DÉFINITIONS

Il importe tout d'abord de distinguer clairement les risques entraînés par un transfert de données des facteurs susceptibles d'avoir une influence sur ce risque.

1.A. Notions de risque et de dommage

Le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage.

Dans le cas des transferts de données personnelles, nous avons classifié les risques en quatre grandes catégories, que nous détaillons ci-dessous: ce sont les risques de perte de contrôle, de réutilisation des données, de manque de proportionnalité et d'inexactitude de ces données.

Les dommages, quant à eux peuvent être d'ordre immatériel, matériel, ou encore concerner la sécurité physique des personnes. Bien que la question de la détermination du type de dommage plus spécifiquement entraîné par la réalisation de l'un ou l'autre des risques identifiés soit examinée en détail ci-dessous, il paraît utile de rappeler brièvement ce que recouvrent ces différentes catégories de dommages.

Le dommage immatériel est une atteinte à la personnalité provenant de la violation d'une liberté ou d'un droit fondamental. Cette violation entraîne par elle-même ce type de dommage, même si il n'y a pas de dommage matériel ni même dommage moral au sens classique du terme. Nous préférons le qualificatif d'"immatériel" à

celui de "moral" car ce dernier nous paraît répondre à des conditions plus strictes, et ne pas être défini identiquement dans toutes les traditions légales. Pour illustrer cette différence par un exemple tiré de la matière étudiée, on peut estimer que l'inclusion d'une personne dans une liste d'adhérents à un parti politique extrémiste constitue un dommage moral, alors que la perte de contrôle sur les données (ne plus savoir qui sait quoi sur soi) représente plutôt un dommage immatériel, même si il n'y a pas de réutilisation de ces données.

Le dommage matériel est le résultat d'une atteinte aux biens d'une personne, ou encore à ses possibilités d'en acquérir, de les accroître ou de les gérer. Il nous semble par exemple que la perte d'une chance d'engagement chez un employeur pour des raisons liées à la connaissance par ce dernier d'informations sur la personne constitue un dommage matériel.

L'atteinte à l'intégrité physique est sans doute plus rare dans ce contexte; elle est constituée par les traitements dégradants, les sanctions pénales injustifiées, voire la mort de la personne concernée. Ce type de dommage peut se produire par exemple lorsque des données personnelles sont traitées dans un pays soumis à un régime totalitaire susceptible de détourner les données en question.

Les trois types de dommages cités ci-dessus peuvent bien entendu apparaître séparément ou simultanément à cause de la réalisation d'un risque. A priori, le dommage immatériel paraît le plus bénin, et le dommage "physique" le plus grave, mais il ne nous paraît pas souhaitable d'établir une véritable gradation en cette matière. En effet, une "échelle" des dommages est toujours sujette à controverses, et risque en outre de conduire à diminuer la prévention des dommages jugés moins graves. Or, cela ne semble pas entrer dans les intentions du législateur communautaire, qui vise à

protéger les "libertés et droits fondamentaux des personnes"[1], indépendamment du type de dommage éventuellement subi.

1.B. Notion de "facteur d'influence"

On appelle "facteur d'influence" ou "facteur de risque" tous les éléments propres à un transfert ou une catégorie de transferts qui sont susceptibles d'avoir une influence sur la probabilité de réalisation du risque, soit qu'ils l'augmentent, soit qu'ils la diminuent.

Parmi ces facteurs, certains sont particulièrement liés au fait qu'il s'agit d'un flux vers un pays tiers (situation politique ou technologique du pays tiers, fait que les données sont rarement collectées directement auprès de la personne concernée), tandis que d'autres sont généralement liés à toute forme de transfert de données (nature des données, type de transfert,...).

1.C. Notion de coefficient pondérateur

On vise ici un élément susceptible de renforcer ou diminuer l'importance du *facteur d'influence*: il s'agit de ce que l'on appelle la "différence culturelle". Cette différence culturelle (entre le pays tiers et l'Union européenne) provient d'une divergence entre les traditions juridique, commerciale, industrielle, sociale, etc,... de différents pays. Cette divergence affecte l'appréhension que les pays ont de différents éléments entrant en compte dans le traitement de l'information et dans la protection des données à caractère personnel.

La "différence culturelle" peut porter sur certains facteurs d'influence et en affecter la portée, d'où l'expression de "coefficient pondérateur". Notons que ce coefficient joue également à propos de l'appréciation de la protection offerte par le pays tiers, en rendant plus ou moins efficaces les réponses que ce pays apporte aux risques.

---

[1] Article 1 de la directive.

Cette notion sera donc exploitée dans les deux parties de l'analyse, mais est expliquée en détail dans le présent chapitre.

1.D. Objet de l'analyse

Le développement qui suit vise à expliquer en premier lieu quels sont les risques (pour la personne concernée) entraînés par un transfert de données personnelles, et à décrire ensuite l'influence possible de "facteurs d'influence" sur l'occurrence d'un ou plusieurs risques. Notons que des risques existent toujours, même lors d'un transfert à l'intérieur de l'Europe; toutefois, on le verra, des facteurs de risque peuvent rendre les transferts vers un pays tiers potentiellement plus dangereux. Enfin, ces facteurs de risque doivent être "pondérés" par le coefficient "différence culturelle", agissant différemment pour chaque facteur.

Le but ultime de cette réflexion est de permettre de dégager par la suite un lien entre l'analyse des risques et celle de la protection nécessaire dans le pays tiers.

SECTION 2. DESCRIPTION DES RISQUES

2.A. Réflexions préliminaires

Le but de cette description est de répondre aux questions suivantes: que risque le citoyen européen, quel dommage pourrait-il subir si ses données personnelles sont transférées vers un pays tiers? La réponse prendra en considération le fait que l'on se place ici dans une perspective abstraite où aucune protection n'existerait dans le pays tiers.

Rappelons que le dommage résultant de la réalisation du risque ne doit pas nécessairement être un dommage matériel (comme par exemple une prise de décision négative d'un organisme de crédit sur base d'informations erronées et non corrigées). La perte de

contrôle sur ses données, l'impossibilité de savoir qui sait quoi sur soi-même, peuvent constituer un dommage moral et non quantifiable qui doit être pris en compte également.

Il est clair qu'en réduisant la notion de risque à un simple risque matériel, on prive la protection apportée par la directive d'une part importante de sa spécificité et de son étendue. Le texte communautaire vise en effet à assurer la protection "des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel"[2]. Or, la protection d'une liberté ou d'un droit fondamental s'exerce en-dehors de la survenance d'un dommage matériel. Un droit fondamental est jugé digne de protection en soi, quelles que soient les conséquences que sa violation entraîne: on n'imagine donc pas de ne protéger le droit à la vie privée que contre des atteintes d'ordre matériel.

2.B. Circonstances possibles de réalisation du risque

Une précision s'impose, à propos des circonstances dans lesquelles un citoyen européen aurait à souffrir des dommages résultant pour lui d'un transfert de ses données vers un pays tiers. En effet, on pourrait objecter qu'un traitement de données dans un pays tiers, même si les finalités sont détournées ou les données inexactes, ne peut causer de dommage (en tout cas matériel) à une personne résidant à une grande distance du lieu du traitement.

Or, le dommage peut se produire, et ce, principalement dans trois cas:

- si les données traitées à l'étranger servent à fonder une décision concernant un citoyen européen (exemple: en matière de

---

2 Article 1 de la directive.

gestion du personnel), à en faire la cible d'une opération de marketing menée au départ d'un pays tiers (exemple: délocalisation de firmes de mailings et de marketing direct, ainsi le cas présenté dans l'introduction de la présente étude), ou encore à rendre accessibles certaines données que la personne concernée préfère garder confidentielles (exemple: le fait que la personne concernée est séropositive, ou a subi un avortement,...);

- si, après avoir été utilisés ou traités (tri, croisement,...) à l'étranger, les fichiers reviennent dans leur pays d'origine, en comportant des erreurs ou des éléments provenant d'autres fichiers et susceptibles d'entraîner une décision discriminatoire ou injuste à l'égard de la personne concernée;

- si la personne concernée voyage dans le pays où les données ont été envoyées (par exemple dans le cadre d'une réservation aérienne), elle peut également subir un dommage (refus de location de voiture, d'octroi d'une assurance-voyage, sur base d'informations contenues dans d'autres fichiers,...).

2.C. Classification des risques

Les risques encourus peuvent synthétiquement être exposés comme suit: il s'agit de la perte de contrôle sur les données, de la réutilisation des données par d'autres personnes ou pour d'autres finalités, du manque de proportionnalité des données et de l'emploi de données inexactes ou obsolètes.

§ 1. Perte de contrôle de la personne fichée sur ses données

Le risque visé ici est celui qui consiste, pour la personne fichée, à ne plus savoir "qui sait quoi" sur elle.

La perte de contrôle sur les données constitue un risque très fort lorsque le transfert est effectué vers un pays tiers; il est certes concevable d'ignorer le sort de données collectées et traitées dans son

propre pays, mais ce risque est plus facilement évitable, dans la mesure où l'on dispose d'une meilleure connaissance des instances ou organisations susceptibles de traiter les données, de l'environnement juridique (entre autres, des possibilités de recours ou de défense),... Par contre, lorsque les données se trouvent dans un pays tiers, dont on ignore la langue et les usages, et qu'elles y sont détenues par une société ou organisation inconnue, le danger de perdre toute maîtrise sur ces données et leurs traitements successifs est supérieur[3].

Notons que la personne fichée ne subit pas nécessairement un dommage *matériel* du fait de cette simple perte de contrôle. S'il ne s'y ajoute ni réutilisation imprévue, ni détournement de finalité, par exemple, le dommage se limite au fait que le citoyen européen est "fiché" en plusieurs endroits sans le savoir.

Par ailleurs, le dommage immatériel peut même dépasser cette simple ignorance sans pour autant devenir quantifiable financièrement. Si par exemple une personne achète une arme, et que son nom figure donc sur une liste d'acheteurs, elle pourrait, par suite de recoupements (effectués par des sociétés de marketing) avec certains fichiers, être introduite dans une liste d'amateurs de revues de chasse. Or, bien qu'elle ne subisse pas dans ce cas de dommage matériel, cette personne pouvait légitimement souhaiter que ses acquisitions dans ce domaine restent discrètes. Si la personne fichée perd le contrôle sur ses données, elle ne peut demander à être radiée de ces listes.

Enfin, il faut rappeler qu'il est important pour la personne fichée de ne pas perdre la maîtrise sur ses informations, mais qu'en outre, c'est la condition sine qua non pour l'exercice d'un contrôle sur les utilisations ultérieures des données, ou encore sur leur

---

3 Il va sans dire que ce danger est également présent dans le contexte de transferts au sein même de l'Union européenne, mais il est efficacement pris en compte par la directive, et entre autres par le prescrit de l'article 28.6 (rôle des autorités de contrôle en la matière).

exactitude ou leur pertinence. Dès lors, on considère que la perte de contrôle peut non seulement être dommageable en soi, mais qu'elle est susceptible d'entraîner en outre des conséquences en matière de détournement de finalités, d'absence de proportionnalité ou d'inexactitude des données, bref, vis-à-vis de l'ensemble des autres risques.

§ 2. Réutilisation des données

On considère que la réutilisation des données constitue un risque lorsqu'elle est effectuée à des fins différentes de celles qui étaient annoncées initialement et incompatibles avec celles-ci (i), ou encore lorsqu'elle est le fait de personnes autres que celles prévues initialement (ou prévisibles initialement), à qui les données ont été communiquées (ii). Notons que ces deux types de réutilisations abusives peuvent facilement se cumuler.

(i) Lorsque les données sont transférées dans le pays tiers, il existe un grand risque que les données soient réutilisées à d'autres fins que celles prévues initialement. Ce risque peut augmenter selon différents facteurs qui seront développés par après. Ainsi, par exemple, le type de destinataire des données est d'une grande importance: s'il s'agit d'un flux intracorporatif de données du personnel, le risque peut être moins grand que lorsqu'il s'agit de données envoyées à une firme de marketing.

Le danger évoqué ici est plus concret que celui de la perte de contrôle; en outre, dans la mesure où l'usage abusif a par hypothèse déjà eu lieu, le dommage immatériel de perte de contrôle se double plus souvent d'un dommage matériel.

Les illustrations pratiques du dommage ne manquent pas dans ce domaine. On a vu dans la partie introductive de cette étude que les systèmes informatisés de réservation aérienne disposent de codes reprenant telle ou telle caractéristique des passagers empruntant les lignes affiliées. Ces codes concernent aussi bien le statut (VIP, mineur non-accompagné) que des caractéristiques telles que "fumeur

ou non-fumeur", "diabétique", "repas musulman", etc... Les codes en question peuvent être transmis aux agences de voyage, ainsi qu'à diverses organisations touristiques travaillant en collaboration avec elles. On imagine sans mal le dommage potentiel si de telles données sont transmises à l'étranger à une compagnie d'assurances, par exemple.

(ii) Même s'il n'y a pas de détournement de finalité, la simple utilisation par un tiers non autorisé, pour une finalité éventuellement identique ou compatible peut constituer un dommage dans certains cas. En effet, si une personne choisit de confier ses données à une organisation, une firme, c'est en vertu d'une relation existant entre elles, relation qui peut impliquer une certaine confiance. Si les données sont utilisées par d'autres personnes et/ ou à d'autres fins, cette relation n'existe plus nécessairement. Par exemple, lorsqu'une personne accepte de confier ses données à une firme de marketing dont elle connaît les pratiques honnêtes et rigoureuses en matière de sécurité, cela ne signifie pas pour autant qu'une autre société, même si elle utilise les données pour une finalité similaire, bénéficiera de la même confiance.

La réutilisation des données dans l'un ou l'autre des cas mentionnés ci-dessus peut causer des atteintes à l'intégrité physique des personnes. Il est imaginable en effet que certains gouvernements utilisent des données de toute nature (données bancaires, listes d'inscrits à une Université) pour trouver la trace d'opposants politiques par exemple, dans un but de répression. Certains facteurs d'influence aggravent ce risque de manière significative (par exemple, situation politique du pays tiers).

En conclusion, on peut estimer que, si le détournement de finalité constitue un risque si important, c'est essentiellement parce que les causes légitimant le premier traitement peuvent être absentes

des traitements ultérieurs. Lorsque les finalités ne sont plus maîtrisées, la réalisation de la balance des intérêts (on reviendra en détail sur ce concept dans le chapitre III de la présente étude) ne peut plus être assurée.

§ 3. Manque de proportionnalité

On parlera de manque de proportionnalité lorsque les données détenues par le maître du fichier excèdent ce qui est nécessaire pour la réalisation de la finalité annoncée, ou ne sont pas pertinentes par rapport à cette finalité.

Lorsque les données sont transférées à l'étranger, et croisées par la suite avec d'autres données issues d'autres fichiers, une société pourrait détenir des données superflues pour le traitement prévu, simplement parce qu'elle a acheté un ensemble de données non triées à cet effet.

Le dommage causé dans ce cas est assimilable dans une certaine mesure à la perte de contrôle: les données personnelles étant considérées comme une part de la personnalité de l'individu, il peut légitimement prétendre à ce que le maître du fichier (son employeur, par exemple) ne dispose pas sur lui de plus de renseignements qu'il n'est nécessaire.

Un dommage matériel est envisageable aussi car on peut trouver parmi les données supplémentaires des critères discriminants. Ainsi, il est fréquent aux Etats-Unis de trouver repris dans un contrat de travail mention de la race de l'employé, ce qui constitue un renseignement non indispensable à l'exécution du contrat, et potentiellement dommageable pour la personne concernée.

§ 4. Utilisation de données inexactes ou obsolètes

On envisage ici l'hypothèse où les données détenues sur la personne fichée sont incorrectes et/ou obsolètes.

Il est préjudiciable à la personne concernée que ses données ne soient pas exactes. En effet, des données incorrectes peuvent entraîner la prise de décisions injustes par l'utilisateur des données erronées, ou encore, de manière plus pernicieuse et incontrôlable, l'inclusion sur une liste noire par exemple (en matière de crédit ou d'assurance,...). Le dommage causé par ces erreurs peut être extrêmement grave et impossible à corriger par la suite, une fois que les données incorrectes ont été répandues (voire même croisées avec d'autres données).

Ici encore, on peut se trouver face à un dommage moral plutôt que matériel. Ainsi, l'inclusion erronée sur une liste de participants à un meeting d'un parti extrémiste peut ne causer aucun dommage matériel, mais il est légitime de vouloir corriger cette erreur.

Notons que dans le cas de la réalisation du risque d'inexactitude des données, la personne fichée n'a pas nécessairement perdu totalement le contrôle de ses données: elle peut parfaitement savoir qui les détient et en quel endroit. Par contre, bien qu'elle réalise que les données détenues ne sont, par exemple, pas exactes ni mises à jour, la personne concernée ne parvient pas à y accéder. Les barrières sont en effet nombreuses lorsque les données se trouvent dans un pays tiers, qu'il s'agisse d'obstacles constitués par la langue, la méconnaissance des institutions et organisations, ou encore de l'impossibilité de se faire aider à établir son droit,...

Cette difficulté d'accès rend problématique la simple connaissance d'erreurs contenues dans les informations, sans parler de leur rectification ou effacement.

SECTION 3. LES FACTEURS D'INFLUENCE

On appelle "facteurs d'influence" ou "facteurs de risque" les facteurs propres à un transfert ou une catégorie de transferts et qui sont susceptibles de jouer de différentes manières sur des risques

mentionnés plus haut. Le plus souvent, les facteurs d'influence peuvent agir dans les deux sens sur les risques, soit pour les aggraver, soit pour les diminuer.

Ces facteurs sont propres à diverses caractéristiques du flux considéré: son destinataire, la nature des données qu'il contient, etc... Certains ne créent ou n'influencent que certains risques, d'autres ont une influence sur tous. Enfin, certains sont relativement aisés à cerner (comme la nature des données contenues dans le flux), tandis que d'autres sont difficilement mesurables (situation socio-politique du pays de destination). Enfin, on peut faire une dernière distinction: certains de ces facteurs sont spécifiques à des flux transfrontières alors que les autres sont potentiellement présents dans tout transfert de données.

On trouvera ci-après une description des différents facteurs de risque, ainsi que le type de risque sur lequel ils ont le plus d'impact. Il faut toutefois garder à l'esprit que tous les risques mentionnés ci-dessus existent en germe dans tous les flux, et que la mention d'un risque "aggravé" n'exclut pas la présence des autres risques. Il faut également tenir compte de ce qu'un facteur peut parfois jouer "à charge" et "à décharge". Par exemple, le facteur du "type de transfert" aggrave les risques si le transfert est effectué via un réseau ouvert, mais le diminue de manière significative s'il s'agit d'un réseau fermé. Nous reviendrons dans la partie de cette étude consacrée à la méthodologie sur les manières de prendre en compte l'action des différents facteurs.

3.A. Facteurs propres aux flux transfrontières

§ 1. Pays de destination

Cela peut paraître un truisme, mais un des éléments les plus importants à prendre en compte lorsque l'on veut évaluer la périculosité d'un flux est la situation socio-politique et technologique du pays de destination. C'est également l'un des facteurs les plus

difficiles à évaluer, et pour lequel on ne peut donner que des points de repère, mais non une réponse ferme, définitive et permanente. En effet, tel pays actuellement stable et sûr, par exemple, peut se révéler dangereux peu de temps après.

Relevons une difficulté supplémentaire: il importe de savoir quel est réellement le pays de destination finale. Si le pays analysé ne sert que de pays de transit, et si les données sont par la suite acheminées vers un troisième pays, l'analyse des risques est faussée (voire inutile).

Lors de l'analyse au cas par cas des flux, il faudra tenir compte de ce problème, tout en gardant à l'esprit qu'il peut être difficile de savoir quel est réellement le pays de destination finale si l'émetteur des données et leur destinataire ne souhaitent pas le faire savoir. Toutefois, certains indices se révèlent fort utiles dans la détermination du pays de destination finale. L'absence d'intérêt économique de l'entreprise réceptrice des données dans l'opération de transfert peut indiquer que le flux ne fait que transiter par ce pays. De même, lorsqu'une entreprise dont le siège est situé en Europe envoie des données à une de ses filiales à l'étranger, on peut raisonnablement penser que les données en question sont destinées à revenir au siège par la suite. Un autre indice peut résider dans la nature des données: si elles concernent par exemple toutes les personnes employées par une société rachetée par un groupe américain, il est vraisemblable que ces données aboutissent en définitive aux Etats-Unis.

Les deux caractéristiques à prendre particulièrement en compte dans le contexte qui nous occupe sont la situation socio-politique du pays tiers et l'état de sa technologie.

a) Situation politique

Le pays de destination est susceptible d'aggraver un risque en particulier dans les hypothèses suivantes:

- si le pays en question connaît des troubles importants (guerre civile, insécurité,...), la sécurité des données n'y sera certainement pas assurée. Dès lors, les risques de perte de contrôle et de détournement de finalité sont accrus.

- Il en va de même si le pays tiers souffre de problèmes de corruption d'une telle ampleur que les règles sociétales, y compris les règles de droit ne sont plus respectées. Dans ce cas aussi, la confidentialité et la sécurité des données ne peuvent être garanties valablement. On peut citer certains pays où les organisations criminelles disposent d'accès[4] à toutes les données bancaires détenues même par les banques privées, et où les pouvoirs publics sont impuissants à contrer ces activités.

- Le pays de destination peut également aggraver les risques s'il est gouverné par un pouvoir totalitaire, disposant sur certains secteurs d'une mainmise complète et sans contrôle possible par une instance extérieure. Ces gouvernements peuvent avoir un accès non seulement à tous les fichiers du secteur public, mais parfois également à ceux du secteur privé (banques,...). Dans ce cas, les risques de réutilisation et de détournement de finalité sont grands. Cela peut même s'avérer très dangereux pour les personnes concernées, dans le cas par exemple où l'on transfère vers un tel pays des renseignements sur l'adresse et les habitudes de vie d'opposants politiques en exil.

---

4 Soit par la corruption, soit par des accès aux réseaux, facilités par des moyens techniques importants.

Notons enfin qu'il est impossible de donner ici une liste de pays "dangereux": il faut en effet tenir compte de l'évolution rapide qui caractérise cette matière. Un pays longtemps instable peut devenir sûr en peu de temps; l'inverse est vrai également.

b) Etat de la technologie

- Retard technologique: certains pays tiers, sans connaître les problèmes aigus mentionnés ci-dessus, peuvent souffrir d'un retard en matière technologique tel qu'il y est impossible d'y assurer la sécurité et la confidentialité des données. Le risque de réutilisation non autorisée y est accru. D'autre part, le retard technologique peut diminuer le risque de croisements avec d'autres fichiers. On reviendra dans la partie de cette étude consacrée à la méthodologie sur la manière d'évaluer les conséquences de ce facteur en tenant compte de son ambigüité.

Rappelons que le retard technologique n'est pas nécessairement une caractéristique de pays en voie de développement: il arrive en effet que coexistent dans un même pays secteurs arriérés et technologie de pointe (une des illustrations les plus frappantes est l'Inde).

- Avancée technologique: un pays doté d'une technologie avancée de traitement de l'information peut également être une destination "dangereuse" pour les données personnelles. Il est beaucoup plus facile dans ce type de pays d'effectuer des croisements avec d'autres fichiers, des tris rapides et perfectionnés etc... Ce critère peut donc aggraver les risques de perte de contrôle, de réutilisation et de manque de proportionnalité. Par contre, il permet un meilleur contrôle de la sécurité des utilisations.

§ 2. Caractère direct ou non de la collecte des données

Un facteur influençant spécifiquement les flux transfrontières de données réside dans le mode de collecte des données: le plus

souvent, elles ne sont pas collectées directement par l'utilisateur du pays tiers auprès de la personne concernée (une exception notable à cette remarque étant le transfert via Internet).

Il peut arriver assez souvent que, sans qu'il y ait un transfert international, le maître du fichier utilise des données non collectées directement auprès de la personne fichée. Ainsi, dans l'exemple donné dans la partie introductive de cette étude, un employeur peut collecter des données relatives à son personnel auprès de supérieurs hiérarchiques des employés, du service médical ou social de l'entreprise,... Mais lorsque les données sont utilisées à l'étranger, cette situation devient nettement plus fréquente car il est difficile et coûteux pour le maître de fichier de contacter directement les personnes concernées. Ainsi, par exemple, une société de vente par correspondance établie aux États-Unis préférera acheter une liste déjà constituée par un intermédiaire qui disposera, lui, des infrastructures nécessaires à la collecte des données.

Le caractère indirect de collecte nous paraît constituer un facteur aggravant parce que nous estimons que les risques de perte de contrôle et de détournement de finalité sont accrus dans ce cas. Il paraît en effet plus aisé de garder une maîtrise sur ses données si elles ont été données dans le cadre d'un rapport sans intermédiaire. Dans cette hypothèse, bien qu'il soit situé à l'étranger, on sait qui est le maître du fichier, de quelles informations il dispose, et quelle est la finalité du traitement.

La collecte de données via Internet ne pose pas nécessairement ce type de problème, puisqu'elle permet à une firme située à l'étranger d'obtenir directement auprès des personnes concernées les informations souhaitées. Ainsi, par exemple, il existe des pages Web destinées à faire la promotion d'un produit, et demandant aux personnes intéressées de s'identifier et de donner des informations sur leur consommation du produit en question: dans ce cas, les personnes concernées sont directement en relation avec un maître du fichier situé éventuellement à des milliers de kilomètres de

l'endroit de la collecte. Cela étant, il peut se poser malgré tout un problème de manque de transparence du maître du fichier. Si ses seules coordonnées disponibles sont ses coordonnées informatiques, il peut être impossible de "remonter" jusqu'à la personne ou société dissimulée par cette adresse. L'emploi de "remailers anonymes" rend le problème plus aigu encore, car il permet de rendre même l'adresse informatique réelle introuvable.

De toute manière, même si le maître du fichier annonce clairement ses coordonnées, il reste un réel danger de perte de maîtrise sur les informations. En effet, on sait ce que le maître du fichier sait (il connaît les informations transmises, augmentées des informations déductibles de l'interrogation: pays d'origine, type de questions posées,...), mais on ne sait ni ce qu'il fera de ces informations, ni à qui il va les transmettre. Contre les apparences, le risque de perte de contrôle est important; il faudra être attentif à ce risque lors de l'évaluation du niveau de protection (et entre autre, être particulièrement exigeant en matière de transparence du maître du fichier. Notons enfin qu'il nous semble que ces transferts, même initiés par la personne concernée, ne sont cependant pas couverts par l'article 26 (consentement); il nous paraît qu'on ne peut parler ici de consentement indubitable, car la personne concernée manque d'informations pour savoir à quoi elle consent réellement.

3.B. Facteurs d'influence généraux

On appelle "facteurs d'influence généraux" les facteurs qui ne nous semblent pas affecter de manière plus significative les flux transfrontières que les transferts nationaux (ou au sein de la Communauté européenne, puisque la directive unifie le système de protection des données). Il est clair, par exemple qu'un facteur comme la situation politique du pays tiers n'a pas sa place dans cette liste.

On y trouvera par contre des facteurs liés aux données, au flux lui-même, aux acteurs, ou encore aux finalités.

§ 1. Facteurs liés aux données

a) Sensibilité des données

On entend par données sensibles au sens de la directive celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et celles relatives à la santé et à la vie sexuelle. Affectent également le risque toutes les données dont on peut déduire (éventuellement selon le contexte) de tels éléments[5]. Les données peuvent être sensibles "par nature", au sens de la directive, ou se révéler dangereuses selon le contexte; l'appréciation du caractère sensible des données doit dès lors se faire au cas par cas.

Le caractère sensible ou non des données entraîne des conséquences en matière de proportionnalité des données: si des données sensibles sont réutilisées, on peut être amené à considérer d'office qu'elles sont non proportionnelles, quel que soit le contexte. Par exemple, si des données médicales sont transférées dans un pays tiers à des fins de recherche, elles seront jugées non proportionnelles pour toute autre utilisation (assurances, marketing, emploi,...). Cela constitue une caractéristique des données sensibles par rapport aux autres: la réutilisation d'une donnée non sensible n'entraîne pas nécessairement un problème de non proportionnalité.

Notons que la sensibilité des données agit d'une façon particulière sur *l'ensemble* des risques. En réalité, elle ne rend pas la réalisation du risque plus probable, mais elle en aggrave les conséquences: si le dommage survient, il est plus grand (la réutilisation de données sensibles, ou leur inexactitude entraînent plus de conséquences dommageables que dans le cas d'autres données).

---

5 Par exemple, la publication des bans avant le mariage est un acte de mise à disposition du public de l'information, mais cela ne veut pas dire que la mention de la situation de famille trouve sa place dans tous les fichiers. Certes, la mention du mariage n'est pas une donnée sensible en soi mais la mention du mariage religieux peut être facteur de risque d'atteinte à la vie privée si elle figure dans certains fichiers.

Ainsi, la réutilisation par un employeur potentiel de données relatives à la santé ou aux opinions syndicales d'un employé, données obtenues par hypothèse dans un tout autre contexte, sont susceptibles d'entraîner des conséquences discriminatoires (discrimination, refus d'engagement,...) pour ce dernier.

b) Nombre de renseignements transférés

On peut penser que plus la masse des données sur une personne est grande, plus le risque est grand. Un risque accru dans ce cas est celui du manque de proportionnalité: plus on dispose de données sur une personne, plus le risque de voir ces données excéder ce qui est strictement nécessaire augmente.

c) Nombre de personnes concernées

Le fait de transférer des fichiers concernant un très grand nombre de personnes (par exemple, toute la population d'un pays) aggrave un risque de perte de contrôle sur ces données. En outre, et ceci est valable pour tous les risques, on peut considérer que si un grand nombre de personnes subit un dommage même minime, le risque est plus grand que si peu de personnes subissent ce même dommage.

§ 2. Critères liés au flux lui-même

a) Fréquence des flux

On peut estimer que la fréquence des flux diminue les risques, dans la mesure où une société qui a l'habitude de recevoir une grande quantité de données adaptera ses structures et sera sans doute mieux organisée qu'une société qui ne reçoit des fichiers qu'occasionnellement. Par exemple, la société peut mettre en place une personne uniquement chargée de traiter les flux alors qu'en cas de flux occasionnels, l'organisation peut être moins bonne.

Le risque concerné peut être la réutilisation des données, éventuellement par une personne non autorisée profitant du manque d'organisation pour intercepter les informations.

Notons que des flux fréquents peuvent diminuer le risque d'inexactitude, dans la mesure où ils favorisent une mise à jour plus fréquente. Cela ne vaut naturellement que pour des flux portant sur les mêmes données.

b) Type de transfert

(i) Les fichiers peuvent être envoyés par différents types de réseaux:

- Les fichiers peuvent être envoyés par réseau interne. Dans beaucoup de cas, les sociétés importantes louent une ligne privée aux opérateurs de télécommunications afin de relier leurs différentes implantations. Une société mère peut être ainsi reliée à ses filiales à travers le monde. Les informations transitent par ce réseau fermé sans gros risques à condition bien sûr que des mesures de sécurité soient bien établies.

- En revanche, si les données sont envoyées via Internet, elles transitent par un réseau ouvert beaucoup plus dangereux. Plus particulièrement, la réutilisation est quasi-inévitable dès que les données figurent sur un site Web. La personne concernée perd alors immanquablement le contrôle sur ses données, à moins de les protéger (cryptage), car des réutilisations sont possibles par tous et en tous lieux.

Le risque accru par les possibilités d'interception de ces données sur un réseau ouvert et/ou mal protégé est celui de la perte de contrôle, et de la réutilisation des données.

(ii) Les données peuvent également être transférées sur des supports plus traditionnels: papier, cassettes, disquettes, etc,... Il

convient alors d'être attentif au risque d'interception de ce genre de supports. Même dans un pays où la technologie n'est pas fort avancée, le détournement ou la copie clandestine d'une liste de données imprimées peuvent être relativement aisés.

§ 3. Critères liés aux acteurs

a) Localisation du fichier central des données hors de l'Union européenne

La localisation du lieu de traitement principal des données (dans ou hors Europe) peut avoir une incidence sur les risques. Si les données sont principalement traitées en Europe (exemple: gestion du personnel d'une société dont le siège est situé en Europe), les flux vers l'étranger seront plus exceptionnels (par exemple, dans le cadre d'une mission temporaire à l'étranger), et, surtout, la personne fichée disposera d'un interlocuteur permanent en Europe. Cela diminue évidemment beaucoup le risque de perte de contrôle.

Le raisonnement inverse est généralement valable lorsque le fichier central des données est situé dans un pays tiers (mais il faut considérer les possibilités offertes par l'article 4 de la directive en matière de présence d'un représentant en Europe).

b) Liens économiques, légaux, sociaux ou professionnels entre les différents acteurs

Si le flux s'intègre dans une relation commerciale ou professionnelle plus générale ou dans des relations entre une société mère et ses filiales, le risque de perte de contrôle est moindre car il y a moyen de retrouver la trace des données auprès d'un interlocuteur européen. En outre, les finalités sont souvent liées (par exemple, gestion de groupes de donneurs d'organes pour les hôpitaux, gestion du personnel ou de la clientèle pour une société et ses filiales,...), ce qui diminue également le risque. Cela étant, on ne peut négliger le fait que, vu la diversification des activités de sociétés importantes dans des secteurs parfois fort divers, le risque de réutilisation au sein du groupe mais pour des finalités différentes

existe. Toutefois, l'avantage d'avoir plus facilement un interlocuteur en Europe nous paraît supplanter cet inconvénient.

c) Secteur d'activité du destinataire

Le secteur d'activité est susceptible d'entraîner une aggravation de certains risques, essentiellement en raison de l'utilisation prévisible des données. Dans certains secteurs, la réutilisation des données, leur commercialisation, leur croisement avec d'autres fichiers sont systématiques, car ces activités sont essentielles au secteur en question. On pense aux sociétés de renseignements en matière d'octroi de crédit, ou encore aux sociétés de courtage de données à caractère personnel, qui amplifient encore le risque car, dans leur cas, la réutilisation est systématique et n'est pas nécessairement limitée à un secteur bien défini.

Les risques accrus sont essentiellement ceux de la perte de contrôle et de la réutilisation.

§ 4. Critères liés à la finalité

a) Cohérence dans les finalités

Si les traitements sont indépendants les uns des autres (par exemple, multinationale vendant certaines données relatives à son personnel à une société commerciale qui l'utilisera pour faire la promotion de ses propres produits), le risque est plus grand que si le flux peut être analysé comme une étape d'un processus plus général (par exemple, multinationale traitant les mêmes données pour ses besoins internes).

Le risque de perte de contrôle et de réutilisation avec détournement de finalité diminue en effet lorsque l'ensemble des transferts et traitements participent d'une finalité unique: gestion du personnel, organisation de voyages,...

b) Durée de conservation des données

La durée de conservation des données[6] pose des problèmes en termes de finalité: le plus souvent, les données sont traitées pour une finalité, et conservées pour une finalité liée (à fins de preuve, par exemple). Or, si les données peuvent être nécessaires pendant un certain temps à la réalisation d'une finalité, leur archivage complet peut excéder ces finalités.

C'est donc principalement un risque de non proportionnalité qui se pose, lorsque la durée du traitement est illimitée: des données adéquates et non excessives pour la réalisation d'une finalité de gestion du personnel, peuvent être légèrement excessives pour un archivage à fins de preuve, et totalement non proportionnelles lorsque même cet archivage ne se justifie plus raisonnablement.

En outre, le risque de réutilisation peut également se trouver augmenté. Ainsi, par exemple, en matière de rencontres sportives (jeux olympiques, par exemple), il peut y avoir des flux de données nominatives à travers le monde pendant un laps de temps limité. Les renseignements concernant les dossiers des athlètes sont envoyés à l'instance organisatrice par les fédérations nationales avant les jeux et le dossier de chaque athlète mentionne le nom, la discipline mais aussi le poids, la taille et éventuellement les résultats de tests anti-dopage. La finalité de ces flux est claire puisqu'il s'agit d'organiser les rencontres sportives mais ces fichiers restent dans les ordinateurs et peuvent servir plusieurs années après pour d'autres finalités.

Notons enfin que le risque d'inexactitude des données augmente corollairement à la durée de traitement, surtout lorsque le flux a été exceptionnel et n'est pas mis à jour régulièrement.

---

6 La durée du traitement est d'ailleurs un des éléments à prendre en compte cités par l'article 25.2 de la directive.

c) Finalité déterminée ou non

Il peut arriver que la finalité du transfert soit mal ou pas définie, mais il nous semble qu'une détermination insuffisante des finalités soit plutôt à craindre dans le contexte de certains transferts par Internet: c'est le cas lorsque l'on laisse ses coordonnées dans un "livre d'or" proposé sur un site Web. Les personnes qui ont parcouru les informations sont simplement invitées à laisser leurs coordonnées et éventuellement une appréciation: la finalité n'est pas définie.

Cela étant, même hors du contexte des transferts par Internet, il est imaginable que la finalité d'un transfert soit suffisamment définie pour être en conformité avec le prescrit de la directive en la matière, mais que cela reste assez sommaire pour entraîner un risque de réutilisation. C'est ce genre de cas que l'on vise ici.

SECTION 4. LE COEFFICIENT PONDÉRATEUR

Tous les facteurs d'influence détaillés ci-dessus peuvent voir leur action renforcée ou diminuée par un coefficient: la "différence culturelle". Cette différence peut provenir de l'appréhension que le pays tiers a des différents enjeux de la protection des données, ou encore, de la "corporate culture" de ce pays, de sa tolérance en matière de pratiques commerciales, etc... Ce coefficient varie évidemment selon le facteur auquel il s'applique: un pays tiers peut avoir une grande habitude des croisements de fichiers, mais des exigences très strictes en matière de traitement des données sensibles, par exemple.

On cite quelques exemples de ces différences d'appréciation:

- des nuances peuvent exister dans la manière de considérer la sensibilité des données, et, partant, les conditions de légitimité de leur traitement.

Non seulement certains Etats peuvent estimer que ne sont pas sensibles les données jugées telles par la directive, mais la simple notion de donnée sensible méritant une protection particulière est loin d'être universellement partagée. Cela peut facilement conduire à un problème dans l'appréciation de la légitimité du traitement de ces données: il est courant aux Etats-Unis de traiter des données médicales dans un but commercial (envoi de publicités pour des traitements pour le diabète ou l'asthme, par exemple) et non seulement pour la recherche. Il peut également y avoir un risque au niveau de la conformité de ces données, par exemple si l'on ajoute à un contrat de travail une mention concernant les opinions politiques ou syndicales d'un employé, chose courante dans certains pays.

- La conception que certains pays ont de la proportionnalité des données peut être fort large, et en outre, les pratiques de traitement peuvent varier considérablement d'un pays à l'autre. Certains ont une plus grande tolérance par rapport aux fusions et mélanges de fichiers, et disposent de fichiers concernant un grand nombre de personnes. Il y est dès lors plus facile d'opérer des croisements de fichiers et d'obtenir beaucoup plus de renseignements que ceux résultant simplement de la collecte. Il faudra donc être attentifs à des facteurs d'influence comme le nombre de renseignements transférés, ou encore le nombre de personnes concernées.

- Les habitudes commerciales d'un secteur (marketing, crédit,...) peuvent justifier que l'on considère avec plus de prudence le transfert de données vers le secteur en question. Si l'on sait que tel ou tel secteur a pour habitude de constituer des listes noires et de les communiquer, sans aucune transparence pour la personne concernée, le facteur d'influence "secteur d'activité du destinataire" verra son poids accru.

On le voit, la "différence culturelle" est en soi extrêmement difficile à évaluer, vu la variété des éléments sur lesquels elle peut porter, et l'ampleur différente qu'elle peut prendre selon les pays,

les secteurs, etc,... Il sera sans doute opportun de faire appel à des experts ayant une connaissance approfondie du pays tiers; nous reviendrons sur cette remarque dans le chapitre IV de la présente étude, consacré à la méthodologie.

Rappelons que ce coefficient pondérateur affecte également notablement le niveau de protection du pays tiers, sa façon de répondre aux différents risques: on y reviendra donc également dans le chapitre III de la présente étude.

CONCLUSION

L'analyse d'un flux s'ordonne autour de quelques grands axes, mis en évidence dans le présent chapitre. Si l'on devait résumer l'analyse en quelques mots, l'on pourrait dire que la présence de facteurs d'influence dans un flux, éventuellement pondérés par le coefficient "différence culturelle", conduit à une probabilité d'occurrence de certains risques lors d'un transfert. Enfin, si ces risques se réalisent, un dommage pourrait affecter la personne concernée. Sous forme d'équation (mais nous sommes conscients de ce que ceci a de simplificateur), on pourrait dire que le risque égale le niveau de dommage multiplié par la probabilité de survenance de ce dommage.

La présente étude identifie et classifie les éléments pertinents de l'analyse d'un flux. L'intérêt de la démarche se situe à la fois au niveau de l'analyse conceptuelle et au plan plus pratique de la méthodologie, comme on le verra dans le chapitre IV de la présente étude.

On relève les points principaux suivants:

- l'identification de quatre types de risques présents dans le contexte des transferts de données personnelles permettra de déterminer l'objet de la protection du pays tiers (voir chapitre III).

- L'analyse des "facteurs d'influence" met en évidence les éléments factuels, précis, à prendre en compte dans l'analyse du flux. On souligne l'ambigüité de la plupart de ces facteurs, qui peuvent souvent aggraver ou diminuer la probabilité de réalisation du risque.

- Le coefficient "valeur culturelle" peut avoir une importance considérable dans l'évaluation de l'importance des facteurs de risque, mais également dans l'évaluation de l'effectivité de la protection offerte par le pays tiers (voir chapitre III).

- Les types de dommages identifiés permettent également de nuancer l'appréciation du risque, comme le chapitre IV l'explique. On rappelle toutefois qu'aucune "échelle" des dommages ne peut être réalisée dans l'absolu, et qu'ici aussi, c'est bien une appréciation au cas par cas qui est nécessaire.

Chapitre III. Le "niveau de protection adéquat"

INTRODUCTION

Après l'analyse des risques, il faut maintenant se pencher sur la notion même de protection adéquate. Celle-ci est en effet centrale pour la protection des données dans le cadre des flux transfrontières au départ de la Communauté européenne. Afin de déterminer le contenu de cette protection, cette étude s'est attachée à déterminer quels étaient les objectifs primordiaux de tout système de protection des données.

Ces objectifs peuvent être synthétisés de la manière suivante. Il s'agit d'assurer aux personnes concernées une maîtrise:

- des données les concernant, et partant, de leur image informationnelle (cette maîtrise est rendue possible grâce au principe de "participation individuelle", que l'on cerne de manière plus détaillée ci-dessous);

- de l'usage qui est fait de leur image informationnelle. Dans l'exercice de cette maîtrise, la personne concernée n'est pas seule en cause: la société exerce également un contrôle sur l'usage qui est fait des données personnelles (voir ci-dessous le "principe de finalité").

Outre cette double maîtrise, on considère que la personne concernée peut attendre de son image informationnelle qu'elle réponde à deux caractéristiques principales:

- l'image informationnelle doit être un reflet exact, fidèle, de la personne concernée;le principe de "qualité des données" (voir ci-dessous) découle de cette exigence.

- Cette image doit être corrélée à l'usage qui en est fait; en d'autres termes, les données ne peuvent excéder ce qui est nécessaire à la réalisation de la finalité du traitement (les données doivent donc respecter un "principe de proportionnalité", détaillé ci-dessous).

On peut constater que ces objectifs se retrouvent en filigrane dans les instruments majeurs de protection des données; en outre, le chapitre II de la présente étude a montré que les risques principaux pour la personne concernée dans le contexte des flux transfrontières, consistaient en des atteintes à ces principes.

C'est donc à partir de ces quatre objectifs principaux de protection des données personnelles qu'il est possible de structurer le contenu de la protection adéquate.

1. La notion de "protection adéquate": approche au cas par cas et fonctionnelle.

La directive européenne invite à une approche au cas par cas de la notion de protection adéquate ainsi que nous l'avons développé dans le chapitre I de la présente étude. L'article 25 nous conduit en effet à prendre en considération "toutes les circonstances relatives à un traitement ou à une catégorie de traitement". Il s'agit donc bien ici d'éviter de fonder l'examen d'un traitement sur des critères prédéterminés qui dispenseraient d'une évaluation individuelle.

L'examen de la protection adéquate doit en outre être abordé de manière fonctionnelle: en recherchant à tous les niveaux, du plus général au plus restreint, ce qui peut faire fonction de protection adéquate. Aussi, c'est bien dans un champ aussi large que possible que l'appréciation des moyens de protection doit s'inscrire. Les dispositions légales comme les règlements professionnels ou encore, parmi bien d'autres, des éléments de fait peuvent être pertinents dans cet examen.

2. Des risques aux principes de fond

Le niveau de protection adéquat est directement lié aux risques existants. Le niveau de protection doit en effet s'apprécier par rapport aux risques entraînés par un transfert de données personnelles vers un pays tiers à l'Union européenne. Les quatre grands risques qui apparaissent dans ce contexte ont été identifiés au chapitre précédent: les risques de perte de contrôle, de réutilisation, de manque de proportionnalité et d'inexactitude des données. Il faut donc que la protection dans le pays tiers couvre ces risques de manière adéquate.

On peut donc diviser cette protection adéquate en différents éléments répondant chacun à un risque déterminé: à chaque risque correspond un principe de fond qui entend répondre à ce risque. Bien entendu, cette distinction des quatre risques et des quatre principes leur correspondant ne saurait faire oublier que tous ceux-ci sont intimement liés les uns aux autres de telle sorte qu'il est difficile, sinon dans un but pédagogique, d'isoler chacun d'eux pour rendre compte de la réalité.

Ces principes, les principes de fond, sont consacrés avec des nuances parfois importantes dans toutes les initiatives de niveau international[1] concernant la protection de la vie privée, notamment la convention 108 du Conseil de l'Europe, la résolution des Nations Unies du 23 décembre 1994, les lignes directrices de l'OCDE et bien sûr la directive européenne. Ces principes de fond protègent les principaux intérêts des personnes concernées et limitent de ce fait l'action des responsables de traitements[2]. Les nuances parfois importantes apportées par les différents textes conduisent à s'interroger sur la façon dont il faut les envisager pour déterminer la protection adéquate.

---

[1] Mais également, bien sûr, dans beaucoup de normes de protection des données prises à un niveau national, ou même sectoriel: lois, décrets, codes de conduite,...

3. Principes de fond et règles d'effectivité

Les principes de fond constituent le "noyau dur" de la protection des données et se présentent donc comme des résultats à atteindre. Une fois le contenu de ces principes déterminé, il reste à s'assurer qu'ils trouvent une mise en oeuvre concrète. Ce sont les règles d'effectivité qui jouent ce rôle. Les règles d'effectivité mettent en place les moyens de garantir *in concreto*, pour les personnes concernées, le respect des principes de fond.

Dans le contexte de la protection des données à caractère personnel, il faut donc bien distinguer deux types d'éléments pour approcher le contenu de la protection adéquate: les principes de fond constituent l'objectif à atteindre pour affirmer qu'il y a protection adéquate. Les règles d'effectivité, elles, constituent les moyens nécessaires à garantir la réalisation de cet objectif. Leur nature, leur qualification et leur nombre importent peu, pourvu que le résultat combiné de leur présence garantisse le respect des principes de fond. Il n'est pas possible de décrire toutes les règles d'effectivité; le propos est plutôt d'établir à la fois quelques points de repère pour leur évaluation et d'analyser les conditions dans lesquelles elles peuvent garantir le respect de principes de fond.

4. Les bénéficiaires de la protection adéquate

Avant d'examiner le contenu et les moyens de la protection dont la directive requiert qu'elle soit adéquate, il faut faire une remarque concernant le champ d'application de cette protection. L'objectif de la directive n'est en effet pas d'exporter son modèle réglementaire hors de ses frontières; son but, au contraire, est de protéger les données des personnes bénéficiant au départ de la protection de la directive, y compris lorsque celles-ci sont envoyées à l'étranger.

---

[2] Rappelons que nous utilisons pour cette étude la même terminologie que celle utilisée dans la directive européenne.

Par conséquent, ce que la directive impose, ce n'est pas une protection s'appliquant à l'ensemble de la population mondiale mais plutôt de garantir aux personnes bénéficiant au départ de la protection de la directive le maintien d'une protection adéquate pour les traitements même non soumis à la directive. De cette façon, si par le biais d'un code de conduite, une entreprise prévoit d'assurer des moyens de protection pour toutes les données concernant des individus reconnus protégeables par la directive, il n'est alors pas nécessaire que le système juridique de ce pays tiers accorde une protection à tous ses nationaux. Ainsi, le responsable d'un traitement pourrait, sans modifier les règles de protection qu'il suit habituellement, réserver aux seules personnes originairement bénéficiaires de la protection, la "protection adéquate" de l'article 25. Une telle différenciation est possible par le biais d'un code de conduite, ou par la nomination d'un représentant en Europe, soumis aux dispositions prises en application de la directive et responsable vis-à-vis de tels bénéficiaires. La simple existence d'un code de conduite ou la nomination d'un représentant ne suffisent toutefois pas à la protection des personnes concernées. Il reste à s'interroger sur l'effectivité de la protection réalisée par ces moyens.

SECTION 1. LES PRINCIPES DE FOND

Les principes de fond sont à la base d'un système de protection visant à assurer aux personnes concernées une maîtrise complète de leur image informationnelle, de ses qualités, et de l'usage qui en est fait. En outre, on l'a déjà relevé ci-dessus, ces principes de fond tendent à prendre en charge les différents types de risques. En effet, chaque principe de fond peut être vu comme la réponse à l'existence d'un risque déterminé. De cette façon, aux quatre types de risques examinés précédemment, correspondent quatre principes de fond, sous réserve de nuances sur lesquelles on reviendra.

Le tableau suivant indique les couples "risque- principe de fond".

Risques	**Principes de fond**
Perte de contrôle	Principe de participation individuelle
Réutilisation	Principe de finalité
Non-proportionnalité	Principe de proportionnalité
Inexactitude	Principe de qualité

Nous sommes conscients de ce que ce tableau constitue une simplification de la réalité car aussi bien les risques que les principes de fond ont des points de rencontre et existent souvent ensemble. C'est donc dans un but pédagogique que les risques et principes de fond ont été formalisés de la sorte; il faut donc bien voir le contenu de ce tableau comme un ensemble réticulaire.

Ainsi, de la même manière que les risques coexistent, et sont parfois des conséquences les uns des autres, les principes de fond interagissent: lorsque par exemple, la définition de la légitimité de la finalité du traitement est faible ou douteuse, le principe de participation individuelle verra son importance renforcée. Il est clair également que, dans la pratique, un risque peut être rencontré par différents principes. Le risque de non-proportionnalité renvoie non seulement au principe de proportionnalité, mais encore, aux principes de finalité et de participation individuelle. Enfin, à l'inverse, un même principe a des correspondances avec différents risques: ainsi, le principe de participation individuelle joue un rôle dans la prévention du risque de perte de contrôle, mais également des risques de non proportionnalité et inexactitude des données.

Notons enfin que l'on peut encore opérer une classification des principes de fond, selon l'acteur qu'ils concernent au premier chef: le principe de participation individuelle vise d'abord la personne concernée, alors que les principes de finalité, proportionnalité et qualité des données concernent d'abord le responsable du traitement.

1.A. Le principe de participation individuelle

§ 1. Du risque au principe

Le risque auquel il doit être répondu ici est, comme on l'a vu, la perte de contrôle du sujet fiché sur les données le concernant, sur son image informationnelle. Il est en effet important que chaque individu sache qui détient quelle information à son sujet. Cela se justifie par la nature même de la donnée à caractère personnel. Elle est une partie de la personnalité de l'individu et est susceptible d'être l'instrument d'un rapport de pouvoir. Rappelons que le risque de perte de contrôle et ses implications sont développés dans le chapitre II de la présente étude.

§ 2. Définition

Le principe de participation individuelle exprime la nécessité de permettre par divers moyens à la personne concernée d'obtenir une information sur l'"image informationnelle" que le responsable du traitement a de lui et, dès lors, d'exercer vis-à-vis de cette image un certain contrôle.

§ 3. Le contenu du principe de participation individuelle

La participation de la personne concernée répond à la volonté des rédacteurs des instruments de protection des données[3], quelle que

---

[3] Le principe de participation individuelle est présent dans des instruments tels les Lignes Directrices de l'OCDE (paragraphe 12), la directive (articles 10 à 12), la Convention 108 du Conseil de l'Europe (article 8).

soit leur qualité (législative, réglementaire ou autre). En effet, le but premier de ce principe est d'octroyer une certaine maîtrise aux individus sur les informations qui circulent à leur propos. Ce que l'on exprime par le principe de participation individuelle implique d'abord la transparence des circuits et des opérations concernant les données à caractère personnel; ensuite, dans certains cas (en particulier lorsque la légitimité d'un traitement est plus contestable), la possibilité d'une participation à la décision concernant le traitement, soit sous forme d'opposition, soit sous forme d'une exigence de consentement préalable.

Nous avons donc scindé l'exposé sur le principe de participation individuelle en ces deux composantes: la "transparence", et la "participation individuelle proprement dite".

a) La transparence

(i) Information passive de la personne concernée

Il s'agit de la possibilité pour les individus d'être informés de l'existence d'un traitement effectué sur les données les concernant. Cette information conditionne la possibilité pour les personnes concernées de demander une information sur un traitement de leurs données personnelles, voire de s'opposer à ce traitement: l'accès et l'opposition ne peuvent être exercés que si les individus ont connaissance du traitement des données les concernant.

(ii) Information sur demande de la personne concernée

Il s'agit ici pour la personne concernée de la possibilité d'obtenir sur son initiative la connaissance des informations la concernant et faisant l'objet d'un traitement. L'accès doit être aisé et, s'il n'est gratuit, d'un prix raisonnable. De plus, la forme sous laquelle il se fait doit être intelligible pour la personne concernée.

Ces deux premiers points constituent des éléments indispensables à l'existence d'une réelle transparence.

Nous avons rappelé que la maîtrise sur les informations était l'un des objectifs de la protection des données. La maîtrise implique, sans s'y limiter, *la prise de connaissance*. Cette dernière constitue la base de la maîtrise qui doit encore être complétée par la participation individuelle proprement dite.

La prise de connaissance, on l'a dit, peut se faire sur demande ou suite à l'initiative du responsable. Ces deux facettes de la transparence ont une grande importance, mais on note que, dans certaines hypothèses, le besoin d'information "passive" de la personne concernée semble davantage nécessaire que la possibilité d'accès. C'est par exemple le cas de certains transferts de données par le biais d'Internet. En effet, lorsqu'une personne doit communiquer son nom et son adresse E-mail pour consulter un site étranger, ce n'est pas l'accès aux données qui est ici essentiel car la personne concernée sait précisément le contenu des données la concernant (c'est elle-même qui les a communiquées). Par contre, l'information par le maître du fichier prend toute son importance car la personne concernée désire obtenir d'emblée des renseignements sur le traitement dont ses données feront l'objet (par exemple qui est le maître du fichier, quelles sont les finalités du traitement, quelle sera la durée de conservation des données,...).

b) La participation individuelle proprement dite

(i) Le consentement

Il s'agit d'offrir aux individus le choix de donner ou de refuser leur consentement à la collecte et, de façon plus générale au traitement d'une ou de plusieurs données les concernant. Ce consentement doit être libre et éclairé, c'est-à-dire que la personne qui donne le consentement doit avoir une connaissance suffisamment précise de tous les éléments concernant le traitement. Par ailleurs, le consentement répond au risque lié au contrôle des finalités car en accordant son consentement, on prend connaissance des finalités du traitement, participant par là-même leur détermination.

(ii) L'opposition

L'opposition offre aux personnes concernées la possibilité de s'opposer pour des motifs légitimes au traitement des données les concernant[4]. Cette possibilité d'opposition sera exercée soit a priori, lors de la collecte par la signification du refus, soit a posteriori après connaissance de l'existence d'un traitement des données.

§ 4. Caractère fondamental du principe

Le principe de participation individuelle a une place particulière parmi les autres principes de fond car il permet à la personne concernée de contrôler l'application effective des autres principes. C'est en effet à partir de la connaissance de l'existence d'un traitement que les personnes concernées pourront contrôler le respect des autres principes de fond. Cette connaissance pourra être obtenue grâce aux divers moyens découlant de la mise en oeuvre du principe de participation individuelle.

La participation individuelle peut être considérée comme découlant directement des Droits de l'homme, étant donné qu'il s'agit de l'expression de la maîtrise par chacun de son image informationnelle. Ce principe relève à la fois du droit de la vie privée et du droit à l'image.

Notons enfin que l'accès est présenté *infra* comme un moyen d'effectivité des principes de fond: il est donc à la fois un principe fondamental, et, en fonction des modalités qu'on lui donne, un moyen d'assurer l'effectivité de tous les principes de fond.

---

[4] L'article 14 de la directive européenne prévoit un droit d'opposition particulier dans le domaine du marketing. Ce droit est alors accordé sans justification nécessaire.

1.B. Le principe de finalité

§ 1. Du risque au principe

Le risque visé est ici la réutilisation des données à des fins autres que celles prévues initialement et incompatibles avec celles-ci.

Les conséquences de ce risque peuvent être importantes. Aussi est-il nécessaire d'une part d'assurer une protection pour éviter que les sujets fichés ne soient pris par surprise par l'utilisation à leur insu des données les concernant pour de nouvelles finalités et d'autre part de s'assurer que les nouvelles finalités soient légitimes.

§ 2. Définition

Le principe de finalité implique la limitation del'utilisation de données à caractère personnel aux seuls traitements dont les finalités sont compatibles avec les finalités légitimes de leur collecte initiale.

§ 3. Traduction multiple du principe

a) La légitimité des finalités

De façon générale, toute action de l'homme doit être légitime. C'est particulièrement vrai lorsque les droits et libertés humaines sont en jeu. Ainsi, tout naturellement, cette exigence de légitimité s'étend également au traitement des données à caractère personnel. La question de l'évaluation de cette légitimité se pose alors. La difficulté réside dans le fait que cette légitimité ne peut s'apprécier à partir de clés d'analyse a priori parce que les standards sont relatifs au pays et à la culture auxquels on est confronté.

On ne cherche donc pas, dans le cadre de la définition de la protection adéquate, à définir un niveau de légitimité utilisable dans le monde entier; on requiert au contraire des exigences plus procédurales.

Pour définir la légitimité, on commence par poser le principe que celle-ci ne peut être évaluée par le seul responsable du traitement: cette évaluation doit être faite sous le contrôle de

personnes extérieures à celui-ci. On distingue trois moyens de reconnaître la légitimité:

- la participation de la personne concernée sous forme d'opposition ou de consentement;

- les procédures collectives. Les procédures collectives recouvrent à la fois le travail des organes investis par la société démocratique et les négociations collectives (conventions collectives conclues avec les travailleurs, les représentants des usagers,...);

- les moyens de contrôle externes. Les moyens de contrôle externes visent à apprécier la finalité du traitement au regard d'une pondération des différents intérêts en cause: celui des personnes concernées, des responsables du traitement, voire de tiers intéressés par ce traitement. Cetta appréciation a priori ou a posteriori suppose la possibilité d'interventions d'organe de contrôle indépendants, ou au moins "neutres" (nous reviendrons sur ces notions de manière détaillée. Voir *infra*).

Il reste que cette légitimité, quelle que soit la source de sa définition, demeure bien sûr susceptible d'être contestée devant des organes judiciaires.

b) Des finalités déterminées et explicites

Afin de permettre l'évaluation de chaque finalité du traitement, il faut que les finalités soient déterminées et explicites. En effet la légitimité ne peut être atteinte que si les finalités sont précisées et ne peuvent faire l'objet de modifications unilatérales. Dans le cas contraire, les finalités seraient susceptibles de fluctuer et il serait dès lors bien difficile de reconnaître ou non la légitimité dans un contexte mouvant soumis à la seule volonté du responsable du traitement.

c) La limitation des utilisations au regard des finalités

Après avoir posé que les finalités devaient être légitimes et par conséquent déterminées et explicites, on peut parvenir au point

essentiel de ce principe: les données ne pourront être traitées ultérieurement de manière incompatible avec ces finalités déterminées, explicites, et légitimes. Cela protège donc les personnes concernées contre les risques de réutilisation de leur données et contribue à leur permettre de conserver une maîtrise sur les données les concernant (ce qui fait apparaître un lien étroit entre les principes de finalité et de participation individuelle).

d) Remarque: les données sensibles

Il faut ajouter que certains types de données nécessitent dans certaines circonstances un degré de protection particulier: ce sont les données sensibles, c'est-à-dire les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle. Compte tenu des risques inhérents à ces données, il est important que le requis de finalité légitime soit apprécié de façon rigoureuse afin que leur traitement soit limité à des situations très précises.

Notons que la question des données sensibles n'est en fait pas différente de celle de l'exigence de finalités légitimes, il s'agit juste d'un degré d'exigence supérieur pour ces données. Certains textes consacrent pourtant un statut particulier à ces données sensibles[5]; mais il nou semble que l'on pourrait parvenir au même résultat par le biais d'une exigence stricte de finalités légitimes. Les Lignes Directrices de l'OCDE mentionnent d'ailleurs "qu'aucune donnée n'est en elle même sensible, mais peut le devenir selon son contexte et l'utilisation qui en est faite"[6].

---

[5] Ainsi l'article 8 de la directive européenne ou encore l'article 6 de la Convention 108 du Conseil de l'Europe.

[6] Commentaires détaillés des Lignes Directrices de l'OCDE, paragraphe 7.

1.C. Le principe de proportionnalité[7]

§ 1. Du principe au risque

Le risque concerné est le manque de conformité, c'est-à-dire que le lien direct entre la finalité du traitement et le contenu ou la nature des données est rompu. Soit les données traitées ou conservées excèdent ce qui est nécessaire à l'accomplissement de la finalité soit les données sont conservées pour une durée excédant celle nécessaire à la finalité.

§ 2. Définition

Le principe de proportionnalité implique de limiter les données traitées aux seules données nécessaires à la poursuite des finalités légitimes. Cela signifie que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles seront traitées ultérieurement. La détention et la conservation de données non corrélées aux finalités augmentent en effet les risques de détournement de finalité.

De la même façon, la durée de conservation doit aussi être en relation avec ces mêmes finalités.

1.D. Le principe de qualité

§ 1. Du risque au principe

Le risque correspondant au principe de qualité est le caractère inexact, incomplet ou non mis à jour des données. Le traitement est adéquat sous tous ses aspects, sinon qu'il porte sur des données incorrectes. Ce risque peut causer, comme on l'a dit, des dommages considérables selon l'utilisation qui est faite des données (par exemple le problème des listes noires), mais il est important de

---

[7] Le principe de proportionnalité est présent dans la Directive européenne en son article 6 ainsi que dans l'article 5 de la Convention 108 du Conseil de l'Europe.

faire remarquer que le dommage existe avant même l'utilisation des données. Un préjudice moral peut en effet exister par le simple fait de l'association d'une caractéristique erronée à son nom et sa personne (Par exemple, un individu subit un préjudice moral par le fait de la présence par erreur de son nom dans une liste de militants d'un parti politique extrémiste, avant même l'utilisation de cette liste).

§ 2. Précision du concept

Afin de couvrir ce risque, il convient donc d'établir une protection *a priori* et pas seulement une protection conséquente à une utilisation dommageable de données inexactes. Le principe de qualité implique plus qu'une simple possibilité de recours.

Il implique avant toute chose une collecte rigoureuse. S'ajoute à cela, dans les cas où la finalité du traitement exige une conservation des fichiers, une mise à jour des données, chaque fois que c'est nécessaire. Même si la difficulté et le prix de cette mise à jour augmentent avec l'éloignement géographique du sujet fiché par rapport au maître du fichier, des efforts raisonnables doivent au moins être fournis en vue de cette mise à jour.

Conclusion

Avec l'examen des principes de fond de la protection des données à caractère personnel, est réalisée la première étape de la définition d'un standard garantissant une protection adéquate des données personnelles. Ce standard est avant tout un contenu correspondant à la protection adéquate qu'il convient d'opposer aux risques existants. Il reste alors à examiner les moyens à mettre en oeuvre pour parvenir à un tel résultat. Ces moyens peuvent être extrêmement divers dans les différents États tiers. Ils sont tantôt juridiques, tantôt non juridiques; tantôt répressifs, tantôt préventifs; tantôt explicites, tantôt implicites. L'essentiel est que ces règles d'effectivité parviennent sans ambiguïté au résultat défini par le corps de principes de fond, à savoir:

* Principe de participation individuelle

* Principe de finalité

* Principe de qualité des données

* Principe de proportionnalité

Ces quatre principes de fond sont retenus parmi les nombreuses possibilités qu'offrent les différents instruments internationaux parce qu'ils semblent constituer la base de la protection adéquate. Dans le choix de ceux-ci, la classification proposée s'écarte pourtant des autres typologies qui ne distinguent pas principe de fond et règle d'effectivité, augmentant alors la liste indifférenciée des principes. Ainsi on retrouve parfois dans les principes le problème de la sécurité qui se trouve placé ici parmi les règles d'effectivité.

Parmi les quatre principes de fond, il apparaît clairement que deux d'entres eux s'imposent comme les éléments essentiels de la protection adéquate: ce sont les principes de transparence et de finalité. On a en effet eu l'occasion de souligner le caractère fondamental du principe de participation individuelle. Car c'est lui qui offre à la personne concernée l'occasion de prendre connaissance du traitement des données le concernant. C'est à partir de là que la personne concernée pourra avoir accès à ses données et par là s'assurer du respect des autres principes de fond, notamment le principe de qualité.

Le principe de finalité a lui aussi une importance toute particulière, en effet, le principe de proportionnalité n'est en définitive qu'un corrolaire de ce premier principe car la proportionnalité n'est établie que par rapport aux finalités du traitement.

Les principes de fond maintenant posés, il reste à examiner l'effectivité de la mise en oeuvre de ces principes car, comme on l'a

dit, les principes de fond,aussi essentiels soient-ils ne sont rien sans les règles d'effectivité leur correspondant.

SECTION 2. L'EFFECTIVITÉ DES PRINCIPES DE FOND: CONCEPTS EMPLOYÉS

2.A. Réflexions préliminaires

§ 1. L'article 25 et l'effectivité

L'article 25, nous l'avons dit, prescrit une protection adéquate. La description à la première section des principes de fond permet de définir le référent de cette protection,. La seconde section précise le « comment » de cette protection, en d'autres termes, les moyens qui permettront concrètement l'obtention du résultat. A ce propos, l'alinéa 2 de l'article 25 renvoie à une vaste énumération de moyens, énumération par ailleurs non limitative: « les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

Du libellé de cet article se déduisent les deux considérations fondamentales suivantes:

(i) la directive n'entend pas réserver au modèle législatif, le concept de protection adéquate. Ainsi, même si un pays ne dispose pas de loi générale de protection des données, il peut offrir une protection adéquate par d'autres moyens... Les règles professionnelles, c'est-à-dire les codes de conduite sectoriels ou même propres à une entreprise pourraient suffire à certaines conditions;

(ii) si les auteurs de la directive témoignent d'une ouverture très large dans l'acception des moyens utilisés pour l'obtention du but, ils exigent cependant que ces moyens soient « *respectés* », en d'autres termes, que les textes, peu importe leur source, soient l'objet d'application effective. On suppose l'existence de mesures de contrôle du respect des principes, et de sanctions en cas de non respect de ces principes, pour que puisse s'exprimer, le cas échéant,

le principe du "recours" de la personne concernée. Cette présupposition nécessite la reconnaissance de véritables droits dans le chef de la personne concernée (voir *infra*)

Ainsi l'article 25 invite à distinguer, pour évaluer l'adéquation de la protection, trois aspects de celle-ci :

- le premier consiste à s'interroger sur *l'origine, le document qui exprime la protection*: la valeur du moyen d'expression dépendra de l'auteur de ce moyen et de son caractère plus ou moins obligatoire et contraignant ;

- le deuxième envisage les *moyens de contrôle* mis en place pour vérifier le respect des principes ;

- le troisième concerne les *moyens de contrainte et de recours* attachés au défaut de respect des principes.

Enfin, on ajoutera que chaque aspect ne peut être étudié séparément et que la valeur d'un moyen dépend bien évidemment des autres moyens qui lui sont annexés.

§ 2. Notion d'effectivité

La question que l'on tente de résoudre ici est la suivante: qu'entend-on par un système "assurant l'effectivité des principes de fond"? Avant de décrire de manière détaillée les moyens de l'effectivité, il convient de mieux cerner cette notion.

L'effectivité se compose de deux aspects, qui renvoient tous deux aux principes de fond préalablement identifiés. Le premier se situe à un niveau général: il s'agit de promouvoir la connaissance et d'assurer le respect des principes de fond. Le deuxième se situe à un niveau particulier: on vise ici la résolution des problèmes divers que peuvent connaître les personnes concernées au regard du traitement de leurs données personnelles.

Si l'on considère qu'une "protection adéquate" est constituée au minimum d'un "noyau dur", il faut donc que non seulement certains principes de fond soient présents dans le pays tiers, mais également que leur respect soit assuré, et que des recours existent pour les personnes concernées en cas de violation des dits principes. Il nous paraît hasardeux de tenter de déterminer lequel des aspects de l'effectivité est le plus important: dans un contexte de flux transfrontières de données, ils sont aussi indispensables l'un que l'autre. On voit mal l'intérêt pour les personnes protégées par la directive de l'existence dans le pays tiers d'une affirmation législative des principes de fond, par exemple, si ces principes ne sont pas respectés et/ou que les personnes éventuellement lésées ne peuvent obtenir réparation.

Les moyens assurant l'effectivité sont présentés en trois parties: les moyens d'expression, de contrôle et enfin, de contrainte et de recours. Les moyens d'expression ont plutôt pour objet d'assurer le versant "général" de l'effectivité (affirmation et mise en oeuvre des principes), tandis que les moyens de contrainte et de recours visent évidemment la résolution des problèmes individuels (quoique les sanctions puissent avoir un effet dissuasif qui les renvoie au premier objectif). Enfin, les moyens de contrôle présentent souvent les deux facettes: ils tendent à assurer la mise en oeuvre des principes, et à permettre certains recours.

2.B. Les concepts de base: moyens d'expression, de contrôle et de contrainte

§ 1. Les moyens d'expression des principes de fond préalablement identifiés

a) Définition

Par « moyen d'expression », on entend le mode écrit ou non, par lequel se trouvent affirmés les principes de fond de la protection des données. Il s'agira tantôt d'une loi globale ou sectorielle, d'un règlement administratif, d'une coutume, d'une normalisation technique, de codes de conduite sectoriels ou propres à une

entreprise[8],... La non exhaustivité de l'article 25 invite à ne rejeter *a priori* aucun de ces modes mais à en évaluer soigneusement l'effectivité en tenant compte de traditions culturelles et juridiques peut-être différentes de celles européennes.

b) Quelques considérations

(i) Parmi les moyens d'expression, on a retenu la certification, la *privacy policy*, le code de conduite sectoriel ou les règles professionnelles et finalement les règles normatives issues de l'autorité publique.

(ii) On distinguera les moyens d'expression suivant l'autorité qui en est l'auteur. Cette classification en apparence simple cache mal quelques difficultés. Ainsi un code de conduite sectoriel émane bien d'un secteur, mais sa valeur, voire l'obligation de le produire et pour chaque membre du secteur de le suivre, peut émaner d'une norme légale ou d'un contrat conclu par les membres du secteur. On ajoutera qu'un moyen d'expression peut se subdiviser en de multiples sous catégories.

Ainsi la règle normative issue de l'autorité publique peut être globale ou sectorielle, émaner de l'autorité législative suprême ou à l'inverse de simples décisions administratives.

c) Classification

Le tableau suivant résume les considérations précédentes.

---

8 Les auteurs de cette étude considèrent qu'un contrat conclu entre l'exportateur et le destinataire des données, et reprenant les principes de fond peut être considéré comme un moyen d'expression, et, en d'autres termes, comme un des moyens envisagés par l'article 25 pour assurer l'adéquation de la protection. Le fait que les mesures contractuelles soient envisagées de manière distincte à l'article 26.2 de la directive n'altère pas cette possibilité. En effet, dans un cas, on considère le contrat comme un moyen de rendre une protection adéquate, et dans l'autre, on le voit comme un palliatif au cas où la protection du pays tiers n'est pas considérée comme adéquate. Cette réflexion ne fera toutefois pas l'objet de plus de développements dans le cadre du présent rapport.

Source d'expression	**Qui exprime?**	**Renvoi possible à d'autres moyens d'expression**
Privacy Policy	Entreprise	Certifications, codes de conduite
Certification	Organe de standardisation	Règles normatives prises par l'autorité publique
Codes de conduite	Organe sectoriel	Règles normatives issues de l'autorité publique
Règles normatives issues de l'autorité publique	¬ constitution ¬ pouvoir législatif ¬ gouvernement ¬ Board	Tous les autres

§ 2. Les moyens de contrôle des principes de fond

a) Définition

Par " moyen de contrôle ", on vise les diverses méthodes (qu'il s'agisse de techniques, de nominations de personnes ou d'institution d'organes), qui ont pour fonction directe ou indirecte, exclusive ou non, de garantir le respect des principes.

b) Une liste non exhaustive

Sans prétendre être exhaustif, on retient les les divers moyens de contrôle suivants:

(i) moyen consistant en l'institution et l'activité d'organes:

l'existence d'une autorité indépendante de contrôle;

(ii) moyens consistant en techniques ou en mesures pratiques:

l'accès par la personne concernée aux données la concernant;

les mesures de sécurité techniques et organisationnelles;

les procédures d'audit externe permettant la certification délivrée par une autorité de standardisation;

les mesures préventives de notification, de déclaration, voire d'autorisation préalable auprès d'une autorité de contrôle, indépendante ou non, ou d'un autre organisme.

(iii) moyens consistant en la nomination et l'activité de personnes:

la nomination d'un « détaché à la protection des données »;

la nomination d'un représentant, au sens de l'article 4.2[9] de la Directive européenne.

---

9 Article 4.2: "Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant sur le territoire dudit Etat membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même".

c) Quelques réflexions

(i) Ces mesures peuvent se combiner. Ainsi la définition de mesures de sécurité n'exclut pas la mise sur pied de procédures d'audit, ou la nomination d'un responsable.

L'accès des personnes, par exemple, si on souhaite lui donner quelque effectivité, s'accompagnera de la nomination d'un détaché à la protection des données, d'un représentant, voire sera garanti par la possibilité d'intervention d'une autorité de protection des données agissant sur plainte de la personne concernée.

(ii) Les mesures de notification auprès d'une autorité de contrôle indépendante ou non, ou d'un autre organisme sont proposées comme moyens de contrôle à côté de l'existence même d'une autorité indépendante de contrôle. Nous faisons volontairement cette distinction car il nous semble que, pour constituer un moyen de contrôle effectif l'existence d'une autorité indépendante de contrôle ne suppose pas nécessairement l'existence d'une procédure de notification. En outre, si cette procédure existe, elle pourrait se faire auprès d'un autre organisme.

Hormis l'audit par une société externe dans le cadre d'une procédure de certification[10], les autres moyens peuvent être retrouvés dans le texte même de la directive :

- la prise de mesures de sécurité « adéquates » est rendue obligatoire par l'article 17 de la directive ;

- l'existence d'une autorité indépendante de contrôle est un élément essentiel de la directive, expressément visé par son article 28; son importance est également soulignée par le considérant n°62 de la directive;

---

10 Cette procédure est vivement recommandée par le modèle canadien (voir infra).

- la nomination d'un détaché à la protection des données peut être une de ces mesures de sécurité prescrites par la directive. On note que l'article 19.2 prévoit que cette nomination dispense le responsable du traitement d'un autre moyen de contrôle, la notification auprès de l'autorité de contrôle;

- l'article 4.2 de la directive prévoit pour le responsable non établi sur le territoire de la communauté mais utilisant des moyens de traitement situés sur le territoire de la Communauté européenne l'obligation de nommer un représentant;

- les articles 10 et suivants détaillent les multiples facettes de l'accès des personnes concernées aux donnée traitées. On rappelle que l'accès est un moyen indispensable de contrôle du respect des principes de fond. Aussi, l'existence de ce moyen de contrôle est-elle essentielle dans l'analyse de l'adéquation de la protection offerte par un pays tiers même si, comme déjà noté (*supra*, Chapitre III), ce moyen de contrôle est inefficace s'il n'est doublé de mesures permettant d'en garantir l'effectivité;

- de nombreuses mesures préalables sont prévues par les articles 18 et suivants. Il s'agit de la notification, des contrôles préalables et de la publicité des traitements. Ces mesures préalables sont exercées par ou auprès de l'autorité de contrôle. On peut les imaginer auprès d'une autre instance administrative voire privée.

d) Critères de présentation des divers moyens de contrôle

Les critères qui pourraient être suivis pour présenter ces divers moyens de contrôle sont doubles. Chaque moyen pourrait être présenté d'une part, du point de vue de celui qui met en place le moyen de contrôle, d'autre part, du point de vue de celui qui exerce le contrôle. A propos de ce second critère, on distinguera:

(i) le contrôle individuel, c'est-à-dire exercé par la personne concernée elle-même. Ainsi, le droit d'accès permet un contrôle individuel.

(ii) Le contrôle par le responsable du traitement, c'est-à-dire que le responsable du traitement assume seul ou avec d'autres le contrôle propre à un moyen déterminé.

(iii) Le contrôle par un tiers

La mise en œuvre du moyen de contrôle peut être le fait d'un tiers par rapport au responsable des données.

Ce *tiers* peut être *non spécialisé* : il s'agira du contrôle soit effectué *par une entreprise* mise en relation d'affaires avec le responsable du traitement, soit effectué *par le public en général* sur base de documents publiés attestant ou non du respect des principes de protection des données. On parlera alors de contrôle collectif diffus.

Le contrôle effectué par un *tiers spécialisé* s'entend soit du contrôle par une *entreprise d'audit* opérant dans le cadre d'une procédure de certification, soit du contrôle organisé par le *secteur* et sous contrôle de celui-ci, soit, enfin, d'un contrôle exercé par une « *autorité indépendante* » même si son activité se réduit au contrôle d'un secteur et est mise en place par le secteur, à condition, que cette autorité jouisse d'une réelle indépendance d'action (voir *infra*).

Sur base des deux critères proposés, on peut classer comme suit les moyens de contrôle retenus.

Moyen de contrôle	**Mis en place par**	**Exercé par**
Mesures de sécurité	Responsable du traitement	Responsable du traitement le cas échéant, contrôle en outre par: - entreprise tierce spécialisée - organe sectoriel - autorité de contrôle
Autorité indépendante de contrôle	Autorités publiques Organe sectoriel	Autorité indépendante de contrôle Organe sectoriel
Accès	Responsable du traitement	Personne concernée le cas échéant (sur plainte): - contrôle par organe sectoriel - contrôle par autorité de contrôle
Détaché à la protection des données	Responsable du traitement	Détaché à la protection des données
Représentant	Responsable du traitement	Entreprise soit représentante, soit tierce
Audit	Responsable du traitement	Entreprise tierce spécialisée Autorité indépendante de contrôle

Notification	Autorité de contrôle Organisme privé	Autorité de contrôle Organisme privé + contrôle collectif diffus

§ 3. Les moyens de recours et de sanction

a) Définition

Par moyens de sanction des principes de fond, on entend, au sens large, les divers modes et procédures de dissuasion, de réparation ou de répression mis en place pour combattre les déviances par rapport aux comportements attendus pour assurer le respect des principes de fond.

b) Objectifs des moyens de sanction

La sanction poursuit deux objectifs : son prononcé poursuit un objectif de réparation ou de répression de dommages, son existence indépendamment de son prononcé, un objectif de dissuasion des infractions. L'aspect dissuasif peut atténuer le besoin de contrôles institutionnels nombreux. On constate ainsi qu'en cas de sanctions pénales très lourdes — comme à Taiwan —, la sensibilisation aux exigences de protection de la vie privée est plus forte chez les responsables du traitement.

Ce qui importe essentiellement dans l'évaluation d'une sanction n'est pas la catégorie déterminée dans laquelle elle se trouve mais plutôt le niveau d'effectivité de la protection dérivée de cette sanction. On sait en effet qu'une sanction disciplinaire peut dans certains cas avoir des conséquences bien plus importantes que des sanctions pénales; l'interdiction d'exercice peut être plus lourde pour une entreprise que la simple amende.

c) Diversité des sanctions

Les modes de sanctions privilégiés par la directive, à savoir les sanctions judiciaires qu'elles soient civiles ou pénales, ne doivent pas faire oublier d'autres modes en provenance d'acteurs différents et dont l'efficacité est indéniable; ainsi l'amende administrative,

l'exclusion d'une association, le refus d'un certificat, le boycottage d'une entreprise, la recommandation, la menace de saisine des autorités judiciaires,...

La sanction judiciaire elle-même ne se réduit pas au seul prononcé de sanctions pénales classiques ou de dommages et intérêts à titre de réparation. Elle peut s'accompagner de mesures de publicité, d'interdiction de traitement, de verrouillage, d'effacement ou de destruction de données,...

c) Classification

Nous proposons de distinguer les sanctions selon leurs auteurs.

Auteurs	**Sanctions**	**Dimension**
Organe de standardisation ou de certification	Refus ou retrait d'un certificat	Nature commerciale
Secteur	Recommandation Blâme, amende, retrait de l'association	Nature commerciale Effets sectoriels si publication Effets vers le public
Autorité de contrôle	Recommandation Destruction de données Interdiction de traitements Avis préalable	Nature commerciale avec effets sectoriels Si publication, effets vers le public

Juridictions administratives	Destruction de données Interdiction de traitements Amendes	Nature administrative Effets vers le public
Juridictions civiles	Réparation du dommage Mesures de réparation en nature Publication du jugement	Nature judiciaire Effets vers le public
Juridictions pénales	Amendes, emprisonnement Réparation du dommage Saisie et destruction Publication du jugement	Nature judiciaire Effets vers le public

2.C. Observations

(i) La diversité des moyens tant d'expression, de contrôle que de sanction ne permet pas une analyse exhaustive de tous les moyens. Le présent exposé en privilégie certains: le choix de ceux-ci s'explique soit par le fait qu'ils sont présentés par des pays tiers comme des alternatives crédibles susceptibles d'assurer une protection adéquate (ainsi la certification et la *privacy policy*), soit qu'ils ont pu faire l'objet d'analyses plus approfondies lors des visites faites dans le cadre de cette étude (la législation taiwanaise avec son système de sanctions pénales), soit encore qu'ils sont suggérés par le texte même de la directive (ainsi le représentant prévu par l'article 4 de la directive, les codes de conduite envisagés à l'article 28).

(ii) Si la présentation distincte des moyens d'expression, de contrôle et de sanctions est voulue pour des raisons de clarté de l'exposé, celle-ci ne peut être poussée trop loin; au contraire, un moyen d'expression renvoie normalement à des moyens de contrôle et de sanctions. Ainsi, une *privacy policy* peut prévoir la nomination d'un responsable et l'application d'une procédure d'audit régulière qui amènera à une certification de son système d'information, ce qui entraînera comme sanction possible, le refus de certification. A l'inverse, il importe lorsqu'on envisage l'existence un moyen de contrôle de connaître la source de sa légitimité, et les contraintes attachées à son défaut. Ainsi, la possibilité d'accès et de rectification reçoit une valeur différente si elle est exprimée par une entreprise volontairement, ou rendue obligatoire par un secteur voire par une législation. Il va de soi que la sanction variera suivant le mode d'expression de ce moyen de contrôle.

(iii) Le propos de la présente partie est donc d'envisager à partir de la définition de chaque moyen, qu'il soit d'expression, de contrôle ou de sanction, quelques réflexions sur leur *effectivité*, en tenant compte des caractéristiques particulières de la dimension "transfrontière" du flux. Le lecteur y trouvera une méthode d'approche de l'analyse de chaque instrument et l'indication des points à discuter ou à vérifier à leur propos. Il s'agit donc tout au plus d'un guide d'évaluation de chaque instrument, compte tenu du fait que la valeur de chaque instrument dépendra des instruments d'autres catégories qui lui sont associés et, bien évidemment, mais nous reviendrons sur ce point, des principes de fond qu'ils consacrent.

2.D. Le "noyau dur" de l'effectivité

§ 1. Les moyens d'expression, de contrôle, et de sanction

Comme on le verra plus en détail ci-dessous, l'effectivité est en général le résultat d'une combinaison de moyens d'expression, de contrôle, et de contrainte. Mais il nous semble important de tenter,

d'ores et déjà, de définir un noyau dur, un ensemble de moyens d'effectivité nous paraissant indispensable en toutes circonstances.

Les éléments formant ce noyau dur sont des moyens de contrôle. Bien sûr, les moyens d'expression et de contrainte/recours doivent être présents, mais il paraît difficile d'affirmer par exemple quel moyen d'expression devrait toujours être là, de déterminer d'emblée une prééminence de l'un sur l'autre. Ceci dit, il est certain que, quel que soit le moyen d'expression choisi, il y ait par lui *création de droit* pour la personne concernée. C'est dans cette seule mesure qu'un contrôle et des recours peuvent légitimement être réclamés. En d'autres termes, le moyen d'expression choisi ne peut être créateur d'un simple devoir moral ou de conscience dans le chef d'un responsable de traitement.

Cette assertion ne nous ramène pas à privilégier la nature réglementaire du moyen d'expression. Certes, lorsqu'il y a législation, ou plus largement, norme édictée par l'autorité publique, la création de droit est automatique, mais le même résultat peut être atteint par bien d'autres voies. Ainsi, le contenu d'un code de conduite précis peut être considéré par les tribunaux comme "règles de l'art" professionnelles, créatrices d'obligations en cas de non respect, même par des entreprises n'ayant pas adhéré à ce code. Une *privacy policy* émise par une entreprise peut, dans la mesure où elle est incorporée à un contrat conclu avec la personne concernée, être créatrice de droits: certains systèmes juridiques voient dans la déclaration publique, ferme et précise d'une politique d'entreprise, une source d'obligations.

Bref, la création de droits peut naître d'une variété de moyens d'expression ou de combinaison de ceux-ci, qui sont chaque fois à apprécier dans le cadre du système juridique de référence, c'est-à-dire, celui du pays tiers où est localisé le responsable du traitement.

En ce qui concerne cette fois les moyens de contrôle, il nous paraît que certains sont indispensables (indépendamment des moyens

d'expression et de recours/contrainte que l'on trouvera dans le pays tiers), car ils sont une condition sine qua non de l'effectivité des principes de fond (que ce soit au niveau général, de mise en oeuvre de ces principes, ou au niveau particulier, de l'assurance d'un recours pour les personnes concernées). La description de ces moyens sera faite de manière plus approfondie ci-après, mais on les cite ci-dessous.

(i) Les mesures de sécurité: une caractéristique essentielle des mesures de sécurité est de limiter l'accès aux données aux personnes autorisées, que ce soit à l'intérieur ou à l'extérieur de l'organisation du responsable du traitement. Or, la nécessité de limiter l'accès est une condition essentielle au respect du principe de finalité.

En outre, la sécurité joue un rôle également vis-à-vis de l'exactitude des données, et peut garantir que l'accès aux données soit proportionnel aux besoins légitimes de chaque utilisateur.

Par ailleurs, c'est dans la mesure où il y a sécurité, c'est-à-dire garantie par le responsable du traitement d'un certain contrôle de l'utilisation des données, que la personne concernée peut avoir confiance dans les dires de ce responsable lorsqu'elle exerce son droit d'accès. En ce sens, la sécurité garantit l'effectivité minimale du principe de participation individuelle.

On le voit, c'est bien ici la première facette de l'effectivité, la mise en oeuvre des principes, qui requiert absolument l'existence des mesures de sécurité, citées d'ailleurs à l'article 25.2 de la directive.

(ii) L'autorité indépendante de contrôle: La situation de la personne concernée face au responsable d'un traitement présente un net déséquilibre. Le rapport de force est inégal entre une personne individuelle et une organisation, soit de part le fait de sa taille et son éloignement, soit de par le fait de la difficulté pour cette personne d'exiger une information loyale sur les traitements le concernant, soit, enfin, de par la crainte du jugement négatif que susciterait une

demande de renseignements auprès du responsable d'un traitement dont on attend un service... Dans le domaine des flux transfrontières s'ajoute au déséquilibre naturel de la personne concernée l'éloignement géographique, la différence de langue ou encore la divergence des systèmes juridiques. Plus encore que pour d'autres, ces flux transfrontières rendent nécessaire d'apporter une certaine aide aux personnes concernées.

Il est donc important d'apporter une certaine aide à la personne concernée, pour quelque peu rééquilibrer le rapport de force. L'existence d'une autorité indépendante de contrôle dotée de compétences étendues (on reviendra sur les notions d'"indépendance" et de "compétences" ci-après) nous paraît indispensable à la fois pour ce rééquilibrage et à la mise en oeuvre des principes de fond. La directive elle-même considère d'ailleurs l'institution d'autorités de contrôles indépendantes comme "un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel"[11].

L'autorité indépendante a une triple action, du point de vue de l'effectivité. Elle facilite l'accès aux données, qui est indispensable à l'exercice de la maîtrise sur ces données; elle a une action de supervision et d'éducation relative aux principes de protection des données. Enfin, elle joue un rôle irremplaçable dans l'application du principe de finalité, en étant l'instance indépendante d'appréciation de la balance des intérêts. Les fonctions d'ombudsman exercée par une autorité indépendante de contrôle ont en outre une importance certaine dans le deuxième aspect de l'effectivité (résolution des problèmes individuels).

- L'accès: l'accès de la personne concernée à ses données est une condition indispensable à la mise en oeuvre du principe de participation individuelle, bien sûr, mais il permet également à la personne concernée d'exercer un contrôle sur le respect de la finalité

---

11 Considérant 62 de la directive.

annoncée du traitement, ainsi que sur la proportionnalité et l'exactitude des données employées. C'est pourquoi il nous semble que l'accès de la personne concernée est un moyen de contrôle essentiel à l'effectivité des principes de fond.

En résumé, on peut considérer que le "noyau dur" de l'effectivité se résume comme suit:

- les principes de fond doivent être exprimés par un des moyens proposés, ce moyen devant être créateur de droits pour la personne concernée;

- des recours et sanctions adaptés au moyen d'expression doivent exister;

- parmi les moyens de contrôle, trois sont indispensables (mesures de sécurité, autorité indépendante de contrôle, accès). Les autres moyens seront plus ou moins nécessaires selon les circonstances entourant le transfert considéré.

§ 2. Flux transfrontières au départ du pays tiers

Une observation s'impose encore au sujet de l'effectivité: une protection considérée comme adéquate peut être privée d'effet si le pays tiers offrant cette protection permet le transfert ultérieur vers un autre pays qui en est, lui, dépourvu. On court alors le risque de voir certains pays tiers dotés d'un niveau de protection adéquat être utilisés comme simple lieux de transit pour les données, qui seraient

alors transférées ultérieurement vers d'autres pays tiers[12]. Cela étant, il s'agit ici d'une hypothèse qui devrait en principe rester marginale, puisque le pays tiers analysé doit être le pays de destination finale. Cependant, il peut arriver qu'après avoir été considéré comme pays de destination finale, un pays tiers soit amené à transférer des données vers un troisième pays de manière tout à fait légitime. Il importe donc de prendre cette éventualité en compte.

Il convient dès lors que les mécanismes de protection du pays tiers règlent cette question, en conditionnant les transferts vers un autre pays à l'offre par ce dernier d'une protection qui puisse également être considérée comme adéquate, au regard des des données considérées. La protection de ce pays devrait donc correspondre au moins au niveau de protection considéré comme adéquat selon l'article 25 de la directive pour le type de transfert en question. Seule cette "transitivité" de la protection adéquate peut en assurer l'effectivité réelle, nous semble-t-il..

SECTION 3. L'EFFECTIVITÉ DES PRINCIPES DE FOND: LES MOYENS D'EXPRESSION, DE CONTRÔLE ET DE SANCTION

Cette section propose une description détaillée des différents moyens assurant l'effectivité des principes de fond, qu'il s'agisse de moyens d'expression, de contrôle ou de recours et de sanction.

3.A. Les moyens d'expression

L'analyse de chaque moyen se compose d'une "définition", et de "conditions d'effectivité"; ces deux points visent à mettre en évidence les composantes et caractéristiques essentielles de ce moyen au regard de l'objectif poursuivi (assurer l'effectivité des principes de fond). On rappelle que les moyens d'expression ne doivent pas

12 Un exemple classique étant le transfert des données par le Québec vers les Etats-Unis.

seulement répondre à ces définitions, mais être en outre créateurs de droits pour les personnes concernées.

Les points intitulés "remarques complémentaires" visent des réflexions spécifiques à l'intérêt du moyen décrit dans le contexte des flux transfrontières.

§ 1. Les privacy policies

a) Définition

Par *privacy policy*, on entend la déclaration publique faite individuellement par un responsable du traitement, contenant des principes de protection des données.

On sait que ce moyen d'expression est prévu par le code de conduite du Canadian Standard Association[13] qui oblige chaque entreprise qui souhaite bénéficier de la certification de l'autorité de standardisation, à promulguer un tel document. La *privacy policy* renvoie alors à un autre mode d'expression: la certification (voir *infra*).

---

13 Il s'agit du point majeur du principe n° 8 dit de "transparence" qui peut se résumer comme suit.
Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.
Ce principe est réputé respecté quand les organisations collectrices de données nominatives énoncent clairement leur politique et leurs pratiques en matière de traitement des informations.
Une personne doit pouvoir obtenir sans effort déraisonnable de l'information au sujet des politiques et pratiques d'un organisme. Ces renseignements doivent être fournis sous une forme généralement compréhensible.
L'organisme peut offrir des brochures à son établissement, poster des renseignements à ses clients, offrir un accès en ligne ou établir un numéro de téléphone sans frais.
Les renseignements fournis doivent comprendre:

a) les nom, fonction et adresse de la personne responsable de la politique et des pratiques de l'organisme et à qui il faut acheminer les plaintes et les demandes de renseignements;
b) le moyen d'avoir accès aux renseignements personnels que possède l'organisme;
c) une description du genre de renseignements personnels que possède l'organisme, y compris une explication générale de l'usage auquel ils sont destinés;
d) une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisme;
e) la nature des renseignements personnels communiqués aux organismes associés.

Il est facile d'imaginer par contre que c'est le responsable du traitement (ou l'administration elle-même) qui décide lui-même sans incitation externe ni sectorielle, ni autre, de se doter d'une telle *privacy policy*.

b) Conditions d'effectivité

Une *privacy policy* pour être effective doit être au minimum précise et complète, publique et, enfin, contrôlée dans son application.

La *précision* et la complétude sont importantes dans la mesure où la description floue d'une politique n'apporte aucune garantie quant au contenu de la protection offerte et aux moyens mis en œuvre ni ne permet de recours devant une autorité compétente. Ainsi, affirmer que l'entreprise souscrit à la recommandation de l'O.C.D.E. ne permet pas de connaître par exemple comment le principe de finalité est concrètement appliqué, auprès de quel service l'accès est possible, ...

A propos d'un contenu minimal des points précis à couvrir, par une *privacy policy*, on se référera utilement au modèle canadien[14].

La *publicité* de la *privacy policy* dans un langage compréhensible est essentielle. En effet, lorsque le responsable de fichier adopte et publie un code de conduite, il devient difficile d'enfreindre ce code tout aussi publiquement ensuite, la pression de l'opinion publique pouvant s'avérer forte. Il s'agit donc ici de contrôle collectif diffus (presse, opinion publique, mouvements de consommateurs,...). Ce type de contrôle peut d'ailleurs être implicitement assorti de sanctions, par exemple, à un niveau marketing, par la modification du comportement des

---

14 Voir C.J. BENNETT, *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association*, Rexdale, Canadian Standards Association, 1995.

consommateurs. A noter, la possibilité également de recours devant les tribunaux pour *"false statement"*.

Le contrôle du respect de la *privacy policy* est, nous venons de le souligner, lié en partie à son caractère public. D'autres paramètres peuvent également être évoqués:

(i) les moyens d'expression associés à cette *privacy policy* :ainsi la *privacy policy* rendue obligatoire pour celui qui entend bénéficier d'une certification (système canadien) ou par un code de conduite fait l'objet de contrôles externes et par là de sanctions.

(ii) Les organes juridictionnels eux aussi peuvent exercer un contrôle sur le respect des *privacy policy;* il faut pour cela que celles-ci soient rédigées d'une façon tout à fait précise et complète. Si cela semble être possible dans certains pays, on ne peut pourtant dire que ce soit partout établi de façon incontestable. Notons que ce contrôle juridictionnel est évidemment facilité lorsque la *privacy policy* est intégrée dans un contrat conclu entre le responsable des données et les personnes fichées (exemple: engagements pris par une banque vis-à-vis de ses clients et intégrés dans les conditions générales des contrats individuels).

(ii) Les moyens de contrôle associés à la *privacy policy*. Il va de soi que le document a d'autant plus de chances d'être respecté qu'il peut faire l'objet d'un contrôle interne par la nomination d'un détaché voire mieux en outre d'un contrôle externe, par une société d'audit, un organe *ad hoc*, etc,...

c) Remarques complémentaires

(i) La vérification de la qualité d'une *privacy policy* comme moyen d'expression "adéquat" de protection peut être facilitée dans le cas de multinationales également implantées en Europe.

(ii) La *"privacy policy"* repose fortement sur le contrôle collectif diffus lié à sa publication.

§ 2. La standardisation

a) Définition

La standardisation est une norme émise par un organe privé ou publique, définissant les qualités techniques et organisationnelles attendues d'un produit, d'un service ou d'un mode de fonctionnement d'une entité et fixant la procédure par l'obtention d'un certificat[15] de respect des exigences ainsi fixées.

Ainsi la standardisation comme moyen d'expression est définie par un organisme externe à l'entreprise, un organisme de normalisation. De la qualité de cet organe dépendra la qualité de ce moyen d'expression, comme sa diffusion et sa crédibilité.

Ce moyen peut être autosuffisant, mais on note qu'il renverra souvent à d'autres moyens d'expression comme des codes de conduite sectoriels ou des *privacy policy*.

L'adoption d'un standard peut être purement volontaire -c'est le système canadien, ou rendu obligatoire de manière générale ou dans un secteur particulier.

b) Conditions d'effectivité

Une standardisation pour être effective doit être *publique*, non *purement technique* et renvoyer à des *moyens de contrôle*.

Une bonne standardisation implique la participation de tous les acteurs intéressés à la définition du standard.

- La *publication* du standard et des conditions d'obtention du standard est importante pour les raisons déjà relevées à propos de la *privacy policy*.

---

15 Il s'agit d'une procédure d'audit dont nous reparlerons à propos des moyens de contrôle (*infra*)

- Le *contenu* du standard ne peut être purement technique. Un contenu purement technique fixant des règles de sécurité est certes appréciable mais ne peut répondre à des questions plus organisationnelles, nécessaires pour résoudre les questions posées par le respect des principes de transparence, de finalité, etc.

- Le renvoi à des *moyens de contrôle* est essentiel:

• Dans le cadre d'une certification, le contrôle effectif est exercé tout d'abord par l'organisme qui attribue le label certificateur. Cette attribution n'est en effet accordée que moyennant la vérification complète de l'adéquation du fonctionnement de l'entreprise au standard. On sera dès lors attentif aux règles déterminant les conditions d'agréation des sociétés qui procéderont à l'audit, à leur exacte mission et à leur pouvoir d'investigation[16].

• Le contrôle est ensuite exercé par le biais de ce que nous avons appelé le contrôle collectif diffus, c'est-à-dire un contrôle de la société en général, dans la mesure où les conditions de certification sont publiées.

• Enfin, le standard pourra être qualifié de « règles de l'art » et de ce fait constituera un référent pour les tribunaux dans leur appréciation de la responsabilité d'une entreprise en matière de protection des données.

- La *qualité du contenu* d'un standard dépendra de la procédure d'adoption de celui-ci. En particulier, il s'agira d'apprécier dans quelle mesure, une réelle participation (par voie de hearing, par constitution de comités *ad hoc*,...) de tous les acteurs intéressés et non des seuls représentants des responsables de traitement a été respectée.

---

16 Notons que le système canadien de certification envisage des audits réguliers (sur une base annuelle).

c) Remarques complémentaires

(i) La standardisation représente un moyen d'expression intéressant dans le cas de flux transfrontières, dans la mesure où le standard est une référence dont la valeur peut être évaluée une fois pour toute et ce pour un grand nombre de flux différents.

L'accessibilité des documents de référence permet par ailleurs un contrôle aisé des Etats membres européens, qui peuvent facilement contacter l'organe de standardisation.

(ii) Les liens tissés au plan mondial entre organismes de standardisation permettent d'espérer un consensus entre ces agences sur la manière de définir et de consacrer les principes de protection des données.

(iii) Le coût élevé pour une entreprise des procédures de certification, c'est-à-dire, de vérification du respect des standards risque de réserver l'effectivité de ce moyen d'expression aux seules grosses entreprises.

(iv) La faiblesse majeure de la standardisation est l'impossibilité ou l'extrême difficulté des recours individuels (sauf à considérer la norme comme une "règle de l'art"). Il conviendra donc d'être attentif à l'éventuel "encadrement" du standard par une législation assurant une possibilité de recours individuel.

§ 3. Les codes de conduite sectoriels

a) Définition

Par code de conduite sectoriel, on entend les règles professionnelles de protection des données, propres à un secteur et définies au sein de ce secteur.

L'article 27 de la directive encourage la rédaction de codes de conduite « destinés à contribuer en fonction de la spécificité des secteurs, à la bonne application des dispositions ... » de la directive.

Dans le cadre de la directive, le code de conduite se conçoit ainsi comme un mode d'expression subordonné aux règles normatives édictées par l'autorité publique. On notera également que la directive prévoit de manière optionnelle un contrôle de leur conformité à la norme supérieure par l'autorité nationale.

Ce système de la directive ne se retrouvera pas nécessairement à l'étranger: les codes de conduite peuvent être autosuffisants, c'est-à-dire ne se référer à aucune norme "supérieure", ni ne faire l'objet d'aucun contrôle externe particulier hormis celui, général, du judiciaire. C'est le système largement répondu aux Etats-Unis[17] et dans d'autres pays où les secteurs trouvent dans les codes de conduite un mode d'expression de la protection des données plus souple et plus adapté aux besoins du secteur.

b) Conditions d'effectivité

L'effectivité d'un code de conduite dépend du *mode ouvert* de son élaboration, de la *représentativité* de l'association, du *caractère public* de son existence et du *caractère contraignant et efficace* des modes de contrôle et de sanctions qui lui sont associés.

(i) La directive elle-même se réfère à la première condition: il importe que le code de conduite ne soit pas l'objet d'une décision unilatérale des seules responsables du traitement. La procédure de confection du code de conduite doit permettre aux diverses catégories de personnes concernées de s'exprimer (ainsi, les associations de consommateurs pour le marketing direct, les employés pour les codes de conduite relatifs à la protection des données dans les relations de travail,... Cette condition se réfère également au principe d'une définition "collective" des finalités (voir *supra*).

---

17 Voir entre autres les codes cités in P. SCHWARTZ et J. REIDENBERG, *Data Privacy Law: A Study of United States Data Protection*, Charlottesville, Va., Michie, 1996.

(ii) La deuxième condition explicitement sanctionnée par le texte du projet de directive concerne la représentativité au sein du secteur des associations qui promulguent les codes. Il s'agit d'éviter que des codes expriment des points de vue minoritaires. Dans la mesure où la directive prévoit des garde-fous par la nécessité d'une conformité aux dispositions appliquant la directive, cette condition se révèle moins indispensable et a pu être abandonnée. A contrario, elle est peut être souhaitable là où le code de conduite n'est pas une norme subordonnée.

(iii) Le caractère *public* de l'existence d'un code de conduite permet, comme nous l'avons dit à propos d'autres modes d'expression un contrôle collectif diffus. Il permet également aux personnes concernées de s'en prévaloir. A ce propos, des références explicites par les entreprises qui adhèrent au code, à son existence et la possibilité d'en avoir copie aisément doivent être prévues.

(iv) Le caractère contraignant et efficace des moyens de contrôle et de sanction associés au code de conduite est sans doute la condition la plus essentielle. Le code de conduite peut prévoir des modes de contrôle et de sanctions propres ou renvoyer à des modes de contrôle et de sanctions externes.

c) Remarques complémentaires

La mondialisation de l'économie crée le besoin de codes de conduite élaborés non plus au niveau d'un pays, ni même d'un continent, mais bien au niveau mondial. L'existence de codes de conduite "mondiaux" ou discutés au sein d'instances internationales comme la C.C.I. permettra, sinon de promouvoir les codes de conduite européens, au moins d'avoir de bons instruments de référence par rapport aux exigences des codes de conduite européens.

§ 4. Les normes issues de l'autorité publique

a) Définition

Sous le vocable "normes issues de l'autorité publique", on regroupe les diverses règles, ayant une portée obligatoire, générales, sectorielles ou spécifiques, ayant pour objet direct ou indirect la protection des données, émises par une quelconque autorité disposant de l'imperium, c'est-à-dire dotés d'un pouvoir réglementaire.

Une telle définition renvoie à l'existence de multiples catégories de normes.

(i) Le premier critère de distinction est la portée de la règle: est-elle générale, sectorielle ou spécifique? A la tradition européenne (directive de l'Union Européenne et convention du Conseil de l'Europe) des lois générales en matière de protection des données, définissant un régime valable pour toutes activités de traitement[18], on peut *opposer*[19] ou *ajouter*[20] des approches sectorielles (ainsi en matière médicale[21], ou pour la question des traitements nés d'opérations de télécommunication dans bien des états), voire spécifiques à une opération particulière[22].

(ii) Le deuxième critère repose sur le caractère direct ou indirect de la protection des données. Ainsi, une législation stricte de type pénal en matière de secret professionnel médical a un impact positif sur la protection des données dans ce secteur. Pour citer un autre exemple, des législations d'accès aux documents du secteur

---

18 A ce propos, lire R. PIPE, *Will Data Protection go global ? Privacy and American Business*, vol. 2, n° 3, oct. 95.

19 Ainsi, la vision américaine qui estime que le recours à la loi doit être limite aux seuls problèmes saillants de protection des données. Sur cette approche législative parcellaire et subsidiaire, lire P. SCHWARTZ et J.R. REIDENBERG, *Data Privacy Law : A study of United States Data Protection*, op. cit.

20 Ainsi, l'approche européenne qui superpose aux législations globales, des législations sectorielles ainsi, le projet de directive en matière de protection des données dans le secteur des télécommunications qui sera bientôt soumis à décision finale.

21 Ainsi, dans nombre d'états des États-Unis ou en Nouvelle Zélande (*Health Information Privacy Code*, 1994).

22 Un exemple typique étant le *Video Rental Privacy Act* américain.

public interdisent l'accès aux documents confidentiels et autorisent les personnes concernées à s'opposer, pour des raisons de protection des données, à la communication de documents.

(iii) Le troisième critère invite à distinguer, parmi les "quelconques autorités", chacune d'elle suivant sa place dans la hiérarchie et sa portée obligatoire. A cet égard, qu'on ne s'y trompe pas, une place élevée dans la hiérarchie ne signifie pas nécessairement une force obligatoire décisive. Le plus bel exemple est celui de la consécration du principe constitutionnel de la vie privée, dans des pays où le contrôle de la constitutionnalité des lois et des actes gouvernementaux n'est pas possible. On ajoutera que la hiérarchie prévue par le système continental européen où le système exécutif est subordonné au législatif n'est pas universel et que dès lors, la hiérarchie et la portée obligatoire des normes dépendent d'une analyse du système juridique de chaque pays.

(iv) La consécration réglementaire, ou mieux, législative, de la protection des données est souvent présentée[23] comme un plus pour la protection des données, le moyen d'expression le plus efficace. Certaines nuances doivent être apportées:

- la consécration législative n'a de valeur que dans la mesure du contenu de la loi. Si la loi se limite à consacrer de manière vague et incomplète la protection des données, on lui accordera peu de crédit.

- La consécration législative prend sa valeur par l'effectivité des moyens qu'elle se donne pour assurer l'obtention de ses finalités. La loi renvoie tout d'abord aux moyens juridictionnels (en particulier pénaux) de son contrôle qu'elle peut mettre en place et dont elle peut assurer une certaine légitimité (cfr. à cet égard, nos réflexions *supra* sur les codes

---

23 Cfr. argument de C. BENNETT, in *Privacy Codes, Privacy Standards and Privacy Laws: the Instruments for Data Protection and What they Can Achieve*, Paper presented to the Conference on "Visions for Privacy: The Search for Solutions.", Victoria, Canada, 1996, May 9-11, p. 11.

de conduite et *infra* sur les autorités de protection des données et leurs moyens d'investigation et de contrôle).

b) Conditions d'effectivité

Au vu de la multiplicité des distinctions introduites par la définition, il ne peut être question de mettre sur le même pied chaque norme mais plutôt d'envisager pour chaque catégorie quelques réflexions:

(i) *à propos de la distinction entre législation globale, sectorielle et spécifique*, on notera qu'une approche sectorielle ou spécifique sans approche globale -si elle a certes le mérite d'approfondir les principes de fond (en particulier, celui de finalité) dans le champ d'application qui est le sien- pose deux types de difficultés[24]:

- le premier est l'incertitude pour un évaluateur externe des limites du champ d'application exact de ce moyen d'expression ;

- le second est la relative inaptitude de cette approche parcellaire par rapport au fait que le marché se désectorialise et que les groupes d'entreprises diversifient leurs activités.

(ii) à propos de la distinction entre réglementations *concernant directement ou indirectement* la protection des données, on sera attentif:

- premièrement à la façon dont ces dernières consacrent l'ensemble des quatre principes de protection des données. Ainsi, une législation sur le secret médical aura certainement à cœur de définir les catégories de personnes habilitées à traiter les données et leur compétence à ce propos (cfr.

---

24 Ces deux remarques visent entre autres les multiples lois américaines couvrent le secteur des télécommunications.

principes de finalité et de proportionnalité) voire la qualité des données. Elle se référera sans doute moins à la participation individuelle du patient.

• Deuxièmement, on analysera le champ d'application de ces réglementations: les dispositions relatives à la confidentialité des dossiers contenues dans les lois d'accès aux documents administratifs permettent tout au plus de régler les questions d'exactitude de données et d'accès des personnes concernées mais ne règlent pas la question de la proportionnalité et, en ce qui concerne la finalité, ne réglementent que la légitimité des communications externes de l'administration mais pas la question délicate de celle des utilisations internes.

• Troisièmement, les réglementations spécifiques ou sectorielles représentent une source plus difficilement accessible par la personne concernée, en particulier lorsqu'elle réside à l'étranger. Devra-t-elle suivant le problème qui l'occupe consulter différentes réglementations, s'adresser le cas échéant à différentes autorités de contrôle? Ainsi, si le nom d'une personne fichée est utilisé par une société de marketing à partir du fichier de sa banque ou de sa société de carte de crédits, quelle législation devrait-elle interroger?

(iii) Le troisième critère est relatif à la classification des autorités ayant pris la réglementation. L'accessibilité plus ou moins grande du contenu de la réglementation peut être fonction de la situation "hiérarchique" de l'autorité: ainsi, le texte d'une Constitution est, en règle générale, plus accessible qu'un arrêté d'application concernant un secteur particulier. A cet égard, on relèvera la grande facilité d'accès et de lecture qu'offrent certains états à l'ensemble de leurs réglementations, notamment via Internet.

(iv) Nous l'avons dit, la valeur d'une réglementation dépend des moyens d'effectivité qui lui sont liés. Une loi non appliquée par les tribunaux ou ne trouvant aucun relais vu la faillite du système

judiciaire, son coût ou son incapacité à intervenir est sans utilité. On se retrouve renvoyé à ce propos à l'analyse du risque propre à la situation politique du pays destinataire.

Par ailleurs, il sera utile d'apprécier les modes de contrôle ou de sanctions propres auxquels la réglementation renvoie et à leur effectivité.

(v) Même si elle répond à tous les critères mentionnés ci-dessus, une législation ne présente d'intérêt pour la protection des données personnelles en provenance de l'Union Européenne que si elle s'applique aux étrangers non-résidents sur le territoire du pays tiers. Il faudra dès lors être attentif à cette question, en vérifiant (le cas échéant dans la Constitution ou la jurisprudence) si la protection offerte par les normes issues de l'autorité publique du pays tiers peut s'étendre aux étrangers.

c) Réflexions complémentaires

Les lois de protection des données prises dans le cadre de l'adhésion à la convention 108 du Conseil de l'Europe sont par définition une garantie d'expression des principes de fond affirmés par la directive.

Cependant, il ne peut être question de déduire de leur existence la certitude d'une protection adéquate. Il reste à vérifier la présence de moyens de contrôle et de sanctions suffisants pour en garantir l'effectivité.

3.B. Les moyens de contrôle

Le point 2.B. de la section 2 distinguait divers moyens de contrôle. Chacun de ceux-ci fera l'objet d'une analyse suivant la classification suivie jusqu'ici:

- définition
- conditions d'effectivité
- réflexions complémentaires

A nouveau, on notera que l'étude de l'effectivité des moyens de contrôle renvoie à d'autres moyens de contrôle, à des moyens d'expression ou de sanctions. L'exposé qui suit analyse en premier lieu les trois moyens de contrôle faisant partie du "noyau dur".

§ 1. Mesures de sécurité

a) Définition

Les mesures de sécurité sont des mesures tantôt liées à la conception ou à l'environnement physique du système informatique tantôt issues de facteurs organisationnels concernant l'exploitation de ce système. Ces mesures de sécurité permettent d'assurer le respect de principes de protection des données lors de leur traitement. On distinguera les mesures de sécurité externes c'est-à-dire protégeant les données contre les accès de tiers[25] et celles internes vis-à-vis des personnes "placées sous l'autorité directe du responsable du traitement ou du sous-traitant".

---

25 Suivant la définition donnée par l'article 1.f) de la directive européenne : "la personne physique ou morale, l'autorité publique, le servise ou tout organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données."

(i) Sécurité externe

Il est important que des mesures de sécurité externe soient prises pour le traitement des données. En effet, pour que les exigences des principes de fond puissent être atteintes, il est nécessaire de s'assurer que les données à caractère personnel ne puissent échapper au responsable du traitement et aboutir illégitimement dans les mains d'un tiers détenteur qui ne bénéficie plus alors de base de légitimation et pourrait par exemple détourner les finalités premières du traitement.

La mise en place de règles de sécurité externe correspond à l'intérêt du responsable du traitement. La valeur économique des fichiers peut être un puissant incitant à prendre spontanément des mesures de sécurité externe. Ceci dit, on attire l'attention sur des domaines plus précaires.

- dans le secteur non marchand et de la recherche, le coût des mesures de sécurité externe et l'absence de sensibilisation à la question aboutissent parfois à des lacunes dans la protection externe;

- le retard technologique de certains pays peut expliquer la difficulté de mise en place des mesures de sécurité;

- l'utilisation croissante des réseaux[26] dans les relations intra- ou inter-organisations oblige à s'interroger sur la sécurité du réseau et des devoirs des opérateurs de réseau ou de services. L'importance de règles de protection des données en matière de télécommunication s'en trouve justifiée.

---

26 On notera que ce n'est pas par hasard que la première directive européenne sectorielle concerne précisément ce domaine, et que c'est sans doute en cette matière que, dans le secteur privé du moins, la première loi "Privacy" sera prise aux États-Unis.

(ii) Sécurité interne

Les mesures de sécurité externe ne doivent pas nous faire oublier la sécurité interne qui poursuit un but proche mais distinct puisqu'il s'agit cette fois d'éviter que des données à caractère personnel ne circulent sans contrôle à l'intérieur d'un organisme ou d'une société. Ne doivent en effet être destinataires de ces données que les personnes habilitées à cet effet (principes de finalité et de proportionnalité). On peut considérer que la nomination d'un détaché à la protection des données (voir *infra*) est un indice d'une bonne définition de mesures de sécurité adéquates et du contrôle de leur mise en œuvre.

b) Conditions d'effectivité

(i) En général, *les mesures de sécurité* se prêtent aisément à une standardisation et à un système de certification qui doivent être fondés sur le principe de la proportionnalité entre le degré de sécurité et des risques à courir.

Qu'il s'agisse de mesures physiques, techniques (en particulier liées à la conception de logiciels), ou organisationnelles, la standardisation apparaît comme la manière souple de tenir compte des avancées technologiques en la matière. On se référera donc aux réflexions ci avant proposées à propos de la standardisation comme moyen d'expression dont le contrôle peut faire appel à un audit externe.

Le responsable du traitement sera bien évidemment sanctionné par le marché s'il ne dispose pas d'un certificat de sécurité et par les juridictions civiles en responsabilité pour ne pas avoir suivi les règles professionnelles en la matière.

(ii) En particulier pour les mesures de sécurité relatives au réseau, on se montrera plus exigeant. Les opérateurs de réseau et de

services doivent être soumis obligatoirement à des règles, qu'elles soient définies par la loi[27] ou par le secteur.

c) Réflexions complémentaires

(i) La standardisation des mesures de sécurité peut être définie au sein d'organes internationaux (I.T.U., I.S.O., etc.). De telles définitions internationales facilitent un consensus mondial en la matière.

(ii) On peut concevoir dans le cadre de traitements opérés par des multinationales (comme dans l'exemple de la banque de données relative aux qualités du personnel cité dans l'introduction de la présente étude) que des engagements précis soient pris contractuellement sur ce point (p.ex. utilisation des lignes louées sécurisées entre les diverses filiales et succursales du groupe, règlement intérieur relatif à l'accès aux données,...).

(iii) Sans être à proprement parler des mesures de sécurité, des lois pénales comme celles sanctionnant l'accès non autorisé à certaines banques de données, sont de nature à contribuer à la sécurité d'un système.

§ 2. Autorité indépendante de contrôle

a) Définition

On appelle autorité indépendante de contrôle les organes qui, qu'ils soient créés sur le modèle européen ou non, ont pour fonctions de:

- promouvoir le respect des principes de fond de la protection des données, tant auprès des responsables de traitement que du public;

---

27 Notons qu'il existe parfois une réglementation spécifique à propos de la sécurité des réseaux et de la protection de la vie privée, ainsi aux Etats-Unis, le Electronic Communication Privacy Act de 1986.

- faciliter l'accès aux données traitées;

- contrôler les éléments légitimant les traitements;

- constituer une possibilité de recours et d'assistance pour les personnes concernées.

En ce qui concerne les diverses formes que peut prendre une autorité de contrôle, ne s'agit pas ici de transposer à l'étranger le modèle des autorités de contrôle européennes. C'est au contraire une approche fonctionnelle qu'il faut adopter. Il est en effet nécessaire de remplir des conditions fonctionnelles et non d'être constitué sous une forme ou un statut déterminé. On peut donc trouver différents types d'organe remplissant adéquatement le rôle d'autorité indépendante. Ces autorités doivent répondre à différentes conditions, détaillées ci-dessous, pour remplir adéquatement leur rôle.

b) Conditions d'effectivité

(i) Indépendance: L'autorité doit pouvoir agir de manière indépendante. Cela implique trois conséquences :

- L'un des indices principaux d'indépendance est à trouver dans la composition même de cette autorité. En effet, un organe créé et fonctionnant au sein d'un secteur peut être considéré comme indépendant s'il comprend dans sa composition des membres extérieurs au secteur, tels que des associations de consommateurs ou encore des représentants d'un organisme de certification indépendant.

- Le fonctionnement de cette autorité doit être transparent. Cela peut notamment impliquer la publication d'un rapport d'activité et une certaine publicité des décisions. C'est particulièrement important pour que puisse s'exercer un contrôle collectif diffus sur le travail de cette autorité. Ce contrôle permet de s'assurer de l'indépendance de l'autorité.

- Afin de pouvoir jouer son rôle avec efficacité et acquérir les moyens réels de son indépendance, cette autorité doit avoir des prérogatives suffisamment étendues, particulièrement concernant son pouvoir d'investigation, qu'elle peut exercer par elle-même ou de manière déléguée.

(ii) Accessibilité: afin de pouvoir jouer son rôle de manière effective, il est important que l'autorité de contrôle soit aisément accessible aux personnes concernées. Cela implique que:

- l'existence de cette autorité doit être rendue publique de façon à ce que toute personne concernée sache qu'elle peut faire appel à celle-ci.

- La saisine de cette autorité doit être aisée. Cette accessibilité doit exister à différents niveaux: tant du point de vue du prix et des délais que du point de vue du caractère compréhensible -sans compétences particulières- de son travail.

(iii) L'effectivité des mesures susceptibles d'être prises par les autorités de protection des données dépend de leurs réelles possibilité et compétence d'action et de la qualité des législation, standards ou autres mécanismes de protection appliqués lors de leur contrôle. On attire l'attention sur les points suivants:

- la *possibilité d'action* d'une autorité de protection des données dépend de ses moyens d'investigation. Il va de soi qu'un staff limité à quelques personnes peut difficilement assumer un contrôle général de tous les traitements existants dans un pays. On sera attentif alors aux relais extérieurs que cet organisme peut avoir dans des secteurs ou grâce à des sociétés de certification chargés de veiller au respect des mêmes standards.

La *compétence d'action* sera réelle si l'autorité dispose de moyens de contraindre les responsables de traitement à subir les mesures d'enquête, et d'incitation suffisamment fortes à suivre les

avis, recommandations ou décisions que ces autorités pourraient prendre. Il va de soi qu'un cadre réglementaire confiant à ces organes des compétences de droit et sanctionnant les infractions constatées par eux apparaît comme un système idéal mais on peut imaginer que par la voie de la publication de rapports ou de communiqués de presse, par l'engagement d'un secteur de sanctionner les responsables défaillants, on puisse obtenir également une compétence réelle d'action.

c) Réflexions complémentaires

(i) Dans le cadre des flux transfrontières, un des intérêts évidents de la constitution d'autorités de protection des données, est la création d'organes-relais "accessibles" et spécialisés pour, d'une part accueillir les demandes européennes des personnes concernées ou des autorités de protection des données, d'autre part, informer ces dernières de l'état de la protection des données dans un secteur ou dans un pays tiers.

(ii) La notion d'autorité indépendante de contrôle s'entend certes des autorités créées par une réglementation publique et ayant une compétence générale[28] mais elle peut englober des organes créés au sein d'un secteur par une fédération professionnelle à condition que ces organes puissent agir indépendamment. Des critères cumulatifs tirés de la composition multiple de cet organe, du mode indépendant de fonctionnement, de la transparence du fonctionnement, et finalement, de son accessibilité aisée pour les

---

28 Ces autorités peuvent être créées sur le modèle européen (Hong Kong) ou être plutôt inspirée des structures locales.
Ainsi le système de la loi taïwanaise promulguée le 11 août 1995, qui attribue de larges pouvoirs aux autorités de contrôle:
Si un maître de fichier (institution publique ou privée) ne répond pas dans le délai fixé ou pas du tout à une demande d'une personne concernant ses données (accès, correction, effacement), la personne fichée peut introduire une réclamation auprès de l'autorité de contrôle (articles 31 et 32 DPL). Cette autorité de contrôle est le ministère titulaire pour les entreprises privées, et une "autorité de supervision" pour les ministères eux-mêmes.
L'autorité de contrôle peut :
¬ initier une enquête au sujet du manquement invoqué ;
¬ donner l'ordre au maître du fichier de corriger telle ou telle conduite ;
¬ imposer une amende à la personne désignée comme responsable au sein de l'entreprise ;
¬ en dernier recours, révoquer la licence de traitement des données.

personnes concernées, permettent d'établir une telle indépendance. L'absence de vérification d'un critère amène par contre à considérer que l'autorité ne peut correspondre à la qualification d'autorité indépendante.

Pour être considérés comme autorité indépendante de contrôle, il importe également que les organes étudiés jouissent des différentes compétences d'une autorité de contrôle (investigation, fonctions d'assistance aux personnes concernées en cas de problème,...). Ainsi, un organisme d'audit, même désigné par le responsable du traitement, pourrait constituer une autorité indépendante, mais ne peut être considéré comme autorité indépendante *de contrôle* dans la mesure où il ne joue aucun rôle diret vis-à-vis des personnes concernées.

Dès lors, une autorité de contrôle peut être créée par un secteur d'activité ou une fédération d'entreprises si les conditions fonctionnelles sont remplies. Il reste néanmoins qu'un organe créé par l'État avec des compétences générales peut avoir une vision plus globale dans son travail qu'un organe sectoriel. Cette vision globale s'avère importante dans le cadre d'une économie de marché aux nombreux échanges intersectoriels.

(iii) Il est possible d'envisager que les attributions de l'autorité indépendante soient dissociées entre plusieurs organes. Ainsi, on peut séparer le rôle de suivi des dossiers qui pourrait être délégué à des autorités existant dans des secteurs spécifiques et le rôle général d'éveil du public à la problématique de la protection des données.

§ 3. L'accès des personnes concernées

a) Définition

Par accès des personnes concernées, on entend l'ensemble des mesures dépendant du responsable des traitements et qui ont pour objet de permettre à la personne concernée d'exercer une certaine maîtrise de son image informationnelle.

Tout comme d'autres moyens de contrôle, l'accès permet la mise en œuvre du principe de participation individuelle, mais, par là même, est nécessaire au contrôle d'autres principes de fond. De même, la nomination d'un détaché ou d'un représentant facilitent indéniablement, comme il sera montré *infra*, la possibilité pour la personne de contrôler la circulation et la qualité de son image informationnelle mais cette nomination a d'autres buts, ainsi le respect des principes de légitimité, de proportionnalité et de qualité des données.

L'accès des personnes concernées peut se présenter selon de nombreuses modalités, qui peuvent être alternatives ou complémentaires:

— *quant au moment de l'information*

• l'information des personnes concernées peut avoir lieu lors de la collecte;

• l'information des personnes concernées peut être préalable ou concomitante au traitement ;

• l'information des personnes concernées peut avoir lieu lors de la communication à des tiers ;

• l'information peut avoir lieu sur demande de la personne concernée.

— *quant à la qualité de l'information*

• l'information peut porter sur les données traitées, la finalité des traitements, les destinataires des données, l'origine des données, la logique qui sous-tend le traitement et les modalités d'accès.

— quant aux possibilités offertes à la personne concernée suite à l'information

Cette information doit permettre à la personne:

• vis-à-vis du traitement, de s'opposer le cas échéant à certains traitements (*opt out*) ou d'y consentir (*opt in*);

• vis-à-vis du contenu, de rectifier les données (problème de qualité des données) ou d'exiger la radiation de certaines (problème de proportionnalité).

b) Conditions d'effectivité

(i) Première condition

L'accès des personnes concernées doit en particulier dans le commerce international renvoyer à d'autres moyens de contrôle.

Nous avons déjà mis en évidence que, vis-à-vis de traitements situés hors Europe, le principe de transparence devrait nécessairement impliquer le droit de ne pas être laissé seul et renvoyer ainsi à l'intervention d'autorités indépendantes de contrôle. D'autres mesures peuvent selon nous également être prises: nomination d'un responsable, nomination d'un représentant, ...

(ii) Deuxième condition

A propos du moment de l'information, l'accès des personnes concernées à propos de traitements opérés par des responsables situés hors de l'Union Européenne à la suite d'un traitement soumis à la directive ne peut se concevoir que lors de la communication à des tiers par le responsable hors Europe (par exemple, lorsque la société qui exploite le système de réservation aérienne communique les données à une société de marketing) *ou* à la demande de la personne concernée.

En effet, le flux sortant d'Europe est soumis à la directive et donc, sauf exception (dans l'hypothèse prévue par l'article 11.2 de la directive), la personne concernée connaît le destinataire extra européen de l'information. Elle peut donc l'interroger sans que celui-ci n'ait le devoir de la prévenir. Le problème se pose à propos d'utilisations subséquentes opérées par des tiers.

(iii) Troisième condition

La *qualité* de l'information à fournir à la personne concernée s'entend au moins de données traitées, de la finalité du ou des traitements opérés par le responsable hors Communauté européenne, et des éventuelles communications opérées par ce responsable. On peut concevoir pour les traitements dont les effets risquent d'entraîner pour la personne concernée un risque de dommage significatif (atteinte à l'intégrité physique, dommage matériel grave,... Voir chapitre II) que des informations supplémentaires soient requises.

(iv) Quatrième condition

Quant aux possibilités offertes à la personne concernée suite à l'information donnée, une règle peut être proposée : il s'agit d'introduire une certaine relation entre les possibilités d'opposition et de consentement et la manière dont les exigences de finalité légitime et de proportionnalité sont définies : moins strictes sont ces exigences, plus les possibilités d'opposition et de consentement doivent être ouvertes. Ainsi, si un pays peut concevoir qu'un traitement marketing destiné à la vente d'automobiles puisse disposer des données relatives à la religion, il est indispensable que l'accès de la personne concernée l'autorise à s'opposer au traitement d'une telle donnée[29].

---

29 Notons que, dans le cas de l'utilisation de données sensibles à des fins de marketing, il est envisageable d'exiger une démarche d'"opt in" de la personne concernée, et de ne pas se contenter de la possibilité d'"opt out".

(v) Cinquième condition

L'exercice de l'accès doit être d'un *coût raisonnable*, s'opérer dans un *délai* raisonnable auprès d'une personne ou d'un service facilement identifiable, consister en la remise de *documents compréhensibles*.

c) Réflexions complémentaires

(i) L'accès aux données est fondamental dans la mesure où il représente une consécration directe du principe de transparence et que l'affirmation de ce principe est décisive pour assurer le respect des autres principes. Ceci suppose que lors de l'examen de l'adéquation, une attention particulière soit portée à ce moyen de contrôle. Il est impératif que celui-ci soit garanti par une combinaison de moyens d'expression, de sanctions et d'autres moyens de contrôle qui le rendent incontournable. Ainsi, s'il est exprimé par un code de conduite, on veillera à ce que ce code dote des autorités indépendantes de contrôle de la compétence d'appliquer des sanctions disciplinaires. On ne peut se contenter ici de simples déclarations relatives à la politique d'une entreprise non sanctionnables ou sanctionnables au terme d'un recours juridictionnel hasardeux et coûteux.

(ii) L'accès aux données peut se concevoir pour les seuls bénéficiaires de la protection de la directive. A ce propos, il pourrait être mis en place par la nomination d'un représentant en Europe auprès duquel il s'exercera et qui disposera de moyens effectifs d'investigations.

§ 4. Le détaché à la protection des données

a) Définition

Par détaché à la protection des données, on désigne la personne physique ou le service compétent à la fois pour vérifier à l'intérieur de l'organisation du responsable du traitement, le respect des principes de protection des données et pour accueillir les plaintes et demandes de personnes concernées.

On peut concevoir que cette nomination soit volontaire (par une *privacy policy*) ou rendue obligatoire dans le cadre de l'adhésion à un code de conduite[30] voire d'une loi.

b) Conditions d'effectivité

Il est important que le rôle et le statut du détaché à la protection des données soient formalisés de façon très précise dans un texte tel qu'une *privacy policy* ou un code de conduite par exemple.

Pour que la nomination du détaché permette de garantir le respect des principes de protection des données, il est exigé que le détaché:

- fasse l'objet d'une désignation largement connue ;
- occupe une place hiérarchiquement bien située dans l'organigramme de l'administration du responsable de données ;
- dispose d'une certaine indépendance ;
- dispose de prérogatives réelles d'investigations au sein de son organisation.

Chaque condition peut faire l'objet de quelques commentaires:

- la désignation publique du détaché est essentielle pour permettre son accessibilité aisée;

---

30 C'est le principe du *Model Code* du C.S.A. canadien qui consacre le titre 4.1., *"Principle 4.1.: Accountability"* en partie à cette question (articles 4.1.1. et 4.1.2).

• la place occupée dans la hiérarchie de l'organisation du responsable des données est une garantie pour les deux conditions suivantes. Elle permet aussi de s'assurer que ses avis, conseils et recommandations auront un certain impact sur les décisions du responsable;

• l'indépendance du détaché signifie que celui-ci n'est pas subordonné aux injonctions des organes dirigeants. Cette indépendance peut être déduite notamment:

- des procédures de nomination;

- de la publicité du rapport que ce détaché rendrait de ses missions;

- de sa participation à des réunions de personnes ayant cette même mission.

• Enfin, l'effectivité de ce moyen de contrôle dépend bien évidemment des compétences d'investigation qui lui sont reconnues. Un détaché sans possibilité d'inspection de dossiers tenus au sein de l'organisation du responsable de données, ne pourra s'assurer du respect réel des principes.

d) Réflexions complémentaires

(i) La formule du détaché convient mal, entend-on souvent, aux petites et moyennes entreprises. Cette assertion est partiellement vraie. En effet, ces entreprises peuvent se grouper, au sein de leurs associations professionnelles ou en-dehors, pour nommer en commun un détaché, chargé de veiller à l'application des prescrits "privacy" dans un groupe d'entreprises.

(ii) L'appartenance de détachés à la protection des données à des groupes sectoriels ou autres dans lesquels participent des détachés européens permet d'espérer une compréhension mutuelle et un consensus autour des principes de protection des données.

(iii) L'existence d'un détaché à la protection des données fournit un interlocuteur aux personnes concernées mais également aux autorités de contrôle du pays du responsable du traitement voire européennes. Il apparaît à la fois comme un organe de contrôle de "première ligne" et un interface avec les autres autorités.

(iv) La nomination d'un détaché à la protection des données se conçoit plus facilement dans des entreprises ayant une certaine surface que dans des petites ou moyennes entreprises.

§ 5. Le représentant

a) Définition

Il s'agit de la nomination, par un ou plusieurs responsables de traitement non soumis à la directive, d'une organisation située sur le territoire de l'Union Européenne chargée de veiller au plein respect des prescrits de la directive européenne à propos de traitements relatifs à des données originairement protégées par la directive, et désormais localisés hors Union Européenne. Deux remarques doivent être faites d'emblée à ce propos.

(i) La formule du représentant est prévue par l'article 4 de la directive lorsque le responsable du traitement non établi sur le territoire de la Communauté "recourt" (*makes use*) à des moyens situés sur le territoire desdits États membres, mais on peut imaginer que la formule du représentant soit appliquée en dehors des cas prévus par cet article.

(ii) Cette formule a le mérite d'offrir et de maintenir la protection de la directive aux seules personnes originairement protégées par la directive. Elle n'oblige pas le responsable du traitement à modifier son comportement vis-à-vis des autres personnes visées également par ses traitements.

La formule du représentant peut s'imaginer soit de manière individuelle, soit de manière collective. Si la formule à laquelle on songe habituellement, est la nomination *par une entreprise* d'une

entreprise avec laquelle est en relation d'affaire ou membre du groupe, on pourrait également concevoir qu'une *fédération sectorielle* (p.ex. le secteur du marketing) conclue avec une autre fédération sectorielle un contrat de représentation.

Un tel moyen de contrôle supposera pour sa mise en œuvre la conclusion d'un contrat qui spécifiera les modalités par lesquelles le représentant exercera le contrôle du respect des prescrits de la directive.

Enfin, on conçoit que la présence d'un représentant en Europe facilite grandement pour la personne concernée l'accès à ses données.

b) Conditions d'effectivité

La nomination d'un représentant doit être portée à la connaissance des personnes concernées. Elle doit faire l'objet d'un *contrat* qui décrira *de manière détaillée les modalités du contrôle par le représentant du respect de la directive et les sanctions en cas de non respect de ces modalités* ou du prescrit de la directive.

Les clauses de ce contrat doivent être portées à leur demande à la connaissance de la personne concernée ou du moins de l'autorité de contrôle.

Quelques commentaires s'imposent à ce sujet.

(i) En l'absence de contrat, on conçoit mal sur quelle base le représentant disposera de réels moyens d'exercer le contrôle des traitements opérés par le responsable.

Ce contrat devra décrire les modalités de ce contrôle; cela peut se faire sous forme d'audit régulier, par un droit d'inspection des fichiers à la demande d'une personne concernée, par la remise d'un état des traitements certifié conforme qui préciserait les données traitées, les finalités de traitement, le destinataire, les interconnexions, etc.

(ii) La connaissance par les personnes concernées de l'existence de ce représentant est essentielle: elle peut être réalisée de diverses manières, en particulier par une mention du nom du représentant outre les informations fournies par l'exportateur des données selon les prescrits de l'article 12 de la directive. Il va de soi que, si cet exportateur est lui-même désigné comme représentant, l'accès à ce dernier sera plus facile.

(iii) L'accessibilité du contenu du contrat n'est pas à négliger pour garantir aux personnes concernées le choix d'exiger le respect de celui-ci . A tout le moins, si secret d'affaires il y a, le contenu du contrat devrait être accessible aux autorités de protections des données.

(iv) Enfin, il y a lieu de prévoir que ce contrat comporte des sanctions en cas de non respect par le responsable du traitement de ses engagements. Ces sanctions peuvent être commerciales (le représentant exportateur des données peut bloquer pour le futur les flux de données) ou civiles (dommages et intérêts à charge du responsable).

c) Réflexions complémentaires

Le système de contrôle opéré par un représentant est une solution qui peut convenir à des responsables de données ne souhaitant pas modifier leurs règles mais acceptant d'offrir aux personnes concernées bénéficiant de la directive le maintien de la protection d'origine.

L'effectivité de cette solution repose sur le rapport de force que peut entretenir le représentant et le responsable. Ainsi, a priori on discréditera le choix d'un représentant qui apparaîtrait comme n'ayant aucun moyen d'action commerciale et économique contre le responsable.

§ 6. L'audit

a) Définition

L'audit constitue une procédure par laquelle un organisme spécialisé procède à la vérification du respect des conditions mises à l'octroi d'un agrément ou d'un certificat.

L'audit est souvent lié à une procédure de certification mais il peut être également une condition de l'adhésion à un code de conduite ou mis en place par une réglementation de l'autorité publique.

Il peut être partiel et ne viser que certaines mesures (en particulier les mesures techniques), ou être plus large et viser le respect de l'ensemble des principes de base.

b) Conditions d'effectivité

La qualité de l'audit dépendra à la fois:

- des qualités de l'"auditeur" ;
- du mandat de l'"auditeur" ;
- du caractère public du résultat de l'audit.

(i) Par qualités de l'"auditeur" on entend la compétence et l'indépendance qui doivent caractériser celles-ci. A cet égard, on sera attentif aux procédures d'agréation des auditeurs qui ne peuvent être le fait des seuls responsable des traitements.

(ii) Le mandat de l'"auditeur" doit permettre le contrôle effectif du respect des différents principes de la protection des données. Tant le suivi des demandes d'accès, la qualité et la pertinence des données traitées, que l'adoption de mesures de sécurité adéquates doivent pouvoir être vérifiés.

(iii) Le caractère public du résultat de l'audit est indispensable si on souhaite que ce moyen de contrôle ait une

quelconque efficacité. C'est la peur de la perte d'un "label" ou la non-obtention d'un "certificat" qui constituent les meilleurs moyens de pression vis-à-vis du responsable du traitement.

c) Réflexions complémentaires

La mise sur pied au plan international de procédures d'audit et de certification, l'existence d'auditeurs agréés internationalement rendront facile la vérification de la qualité de la protection offerte par les responsables de traitement qui satisferont aux conditions de cet audit[31].

§ 7. Les moyens de contrôle préventifs à disposition d'autorités sectorielles ou de protection des données

a) Définition

Par moyen de contrôle préventifs à disposition d'autorités de protection des données, on entend l'ensemble des mesures préventives que peuvent prendre, ordonner ou déléguer des autorités de protection des données, *qu'elles soient indépendantes ou non.*

Ces mesures préventives peuvent consister en des mesures de mise à disposition d'informations, de notifications, déclarations, ou contrôles a priori des traitements opérés par certains ou par l'ensemble des responsables de traitement.

Ces mesures sont le fait d'autorités de protection des données, c'est-à-dire d'organes spécialement créés pour garantir la protection des données. Ces autorités seront tantôt *indépendantes*, tantôt *dépendantes*, tantôt *sectorielles*, tantôt à *compétence générale.*

---

31 A ce propos, les réflexions de C.J. BENNETT, *An international Standard for Privacy ?*, Paper presented to the CFP'96 Conference, Boston, Mass., March 96. L'auteur plaide pour la constitution de Standards ISO.

b) Conditions d'effectivité

(i) L'effectivité des mesures susceptibles d'être prises par les autorités de protection des données dépend de leur réelle possibilité et compétence d'action et de la qualité des standards ou protections appliqués lors de leur contrôle. On renvoie à ce qui a été dit à ce sujet pour les autorités indépendantes de contrôle, tout en gardant à l'esprit que les mesures préventives peuvent être prises par des autorités ne répondant pas au requis d'indépendance.

c) Réflexions complémentaires

(i) Dans un contexte de flux transfrontières, l'existence d'autorités de contrôle, qu'elles soient indépendantes ou non, constitue un point positif, vu les liens que ces autorités peuvent établir avec les autorités de contrôle européennes.

(ii) Les mesures a priori permettent d'intervenir préventivement; en agissant en-dehors de tout contentieux, on peut aboutir à des solutions négociées donnant des remèdes généraux et non en réponse à un cas individuel. On évite de la sorte la multiplication de problèmes individuels.

3.C. Les moyens de recours et de sanction

Nous avons vu plus haut que la possibilité de recours effectif était une condition fondamentale de l'effectivité pour la personne concernée. Nous nous bornerons dans le cadre de la présente section à quelques considérations relatives au tableau des sanctions proposé au début de la présente section, et aux conditions d'effectivité des moyens de sanction que l'on y mentionne.

Une première réflexion est *l'analyse des conditions de saisine de l'autorité* en charge de la mise en œuvre de la sanction. Le caractère public de cette autorité et le coût raisonnable voire gratuit tant de la saisine que de l'instruction par cette autorité sont indispensables. On ajoutera que le recours collectif (via une association de consommateurs ou via une association de défense des

libertés[32]) facilite encore l'effectivité de la protection. Enfin, le fait de ne pas avoir à démontrer l'existence d'un dommage accroît les possibilités de recours des personnes concernées[33].

Une deuxième réflexion porte sur les conditions procédurales de l'instruction du dossier et du prononcé de la sanction. Peu importe l'autorité en charge du prononcé de la sanction, il importe que l'audition du plaignant, la motivation de la décision[34] et *son caractère public*[35] soient assurés. Les délais exagérés entre la saisine et le prononcé apparaissent également comme des éléments négatifs lors de l'appréciation de l'effectivité d'un recours et des sanctions y liées.

Troisième réflexion, le *degré d'effectivité d'une sanction n'est pas nécessairement liée à l'autorité qui le prend.* La sanction que représente l'exclusion d'une fédération professionnelle peut être beaucoup plus effective qu'une simple condamnation à des dommages et intérêts prononcée par un tribunal civil.

La quatrième réflexion rejoint la troisième: *l'effectivité d'une sanction ne peut être déduite de sa seule nature.* Une sanction de type judiciaire comme une condamnation à des dommages et intérêts n'a

---

32 Dans le cas de flux transfrontières, en particulier, la question se posera d'une possibilité ou d'un droit d'action de l'autorité européenne de contrôle du pays de la personne concernée.

33 Ainsi, selon la loi taïwanaise, toute personne peut demander des dommages et intérêts au responsable de la violation de la loi, même si elle n'a pas souffert de dommage pécuniaire, ni d'atteinte à sa réputation (dans ce cas, une action supplémentaire est prévue).

34 A cet égard, la règle procédurale extrêmement favorable instituée par le système pénal taïwanais, impliquant un renversement de la charge de la preuve.
Pour s'exonérer de sa responsabilité, une institution publique doit prouver que le dommage est dû à un cas de force majeure, un accident, ou un fait du prince (article 27 DPL). Une institution non publique doit prouver en outre qu'il n'y a eu de sa part ni faute ni intention de nuire (article 28 DPL).
La procédure pénale semble donc très favorable aux citoyens :
¬ elle est (en principe) rapide, entre autres car il n'y a pas de système de jury ;
¬ un procès pénal peut être lancé par une personne privée, même sans intervention du ministère public ;
¬ la rédaction de la DPL laisse penser qu'il existe une présomption de faute dans le chef du responsable du traitement, en tout cas dans le secteur privé, puisqu'il lui appartient de prouver qu'il n'a pas commis de faute et n'avait pas d'intention méchante.

35 Etant bien entendu que la publicité de la décision ne doit pas permettre d'identifier le plaignant, à moins qu'il n'y consente.

pas nécessairement plus d'effets qu'une simple recommandation émise par une autorité de protection des données.

Il est donc utile d'analyser attentivement la sensibilité d'un marché et d'une population vis-à-vis des diverses sanctions possibles. Que peut produire comme effet auprès de la population un retrait du label *"privacy conform"* ? Dans quelle mesure, un contrôle collectif diffus existe vis-à-vis de recommandations prises par une autorité de protection des données et dont le texte est publié par la presse ? Plus généralement, l'accès à la justice est-il rendu d'une quelconque manière plus aisé (programmes de *legal aid*, etc...)... Ces questions renvoient bien évidemment à la notion de "différence culturelle" développée plus haut.

Les cinquième et sixième réflexions visent les *sanctions pénales*. Des poursuites pénales pour des faits commis à l'étranger peuvent être déclenchées par les victimes (les personnes concernées) dans leur pays en même temps qu'elles peuvent être ouvertes dans le pays du responsable des données, si une infraction y est également commise. Cette double incrimination autorise, si les pays en ont convenu ou le décident, des collaborations policières entre États. Cette collaboration représente une facilité indéniable pour la personne concernée qui peut trouver dans le relais des autorités policières de son pays une assistance adéquate pour la protection de ses données.

Par ailleurs, la lourdeur des sanctions pénales (interdiction de traitements, emprisonnement des dirigeants) peut jouer un rôle d'incitant important pour le respect des principes de protection des données par les responsables de traitements[36], sauf à conclure qu'une

---

36 C'est en tout cas, le pari fait par les autorités taïwanaise qui facilitent par divers moyens le recours à la procédure pénale. Ceci amène certaines critiques de la part des responsables de traitement: les sociétés utilisatrices de données estiment que la facilité de la procédure pénale risque d'entraîner de grosses difficultés. D'une part, les personnes concernées n'utiliseront plus la procédure "administrative" par le biais de l'autorité de contrôle, car la procédure pénale permet d'obtenir une réparation financière, ce qui est plus intéressant. D'autre part, ces sociétés peuvent craindre que des personnes ou des associations ne se "spécialisent" dans les procès "vie privée", vu la facilité de la procédure. Cela constitue évidemment une menace

telle lourdeur la rendra inappliquée par les tribunaux qui en craindront la démesure.

Les *possibilités d'intervention des juridictions civiles et pénales* font l'objet d'une septième réflexion. Leurs possibilités d'intervention sont liées aux règles de droit qu'elles sont chargées d'appliquer et aux sanctions y reprises. Il va de soi qu'il faut se référer pour évaluer l'intérêt de leurs interventions au contenu des règles normatives de protection des données prises par l'autorité publique. Ce contenu peut être *étroit* : par exemple, le juge pénal ne pourra incriminer que des infractions relatives au secret professionnel ou relatives à l'accès illégitime à des banques de données; ou encore, le juge civil ne disposera que de règles sectorielles,... Certes, on peut parfois se référer à des règles générales telles que celles relatives à la responsabilité pour non respect des règles de l'art, par exemple, mais il sera utile d'en évaluer l'effectivité du point de vue de la protection des données (sanctions adéquates, accès difficile à la jurisprudence, etc.).

Ensuite, la mesure des possibilités d'intervention des juridictions dépend d'une évaluation en général du contrôle juridictionnel du pays, voire de sa situation socio-politique en général. On se référera à ce propos aux considérations décrites *supra* dans l'analyse des risques.

Enfin, une dernière réflexion concerne l'existence de mécanismes d'actions collectives, ou d'actions d'intérêt collectif.L'intérêt des "actions d'intérêt collectif" est bien réel dans le contexte du traitement des données personnelles, lorsque les intérêts individuels en cause ne sont pas suffisants pour fonder une action mais que malgré tout, il existe un intérêt collectif à agir, au nom de la société ou d'une part importante de celle-ci. La France et le Brésil, entre autres, connaissent sous diverses formes ces "actions

---

assez sérieuse pour les sociétés, surtout à cause de la "présomption de culpabilité" qui pèse sur elles.

d'intérêt collectif". Ce mécanisme pourrait jouer un rôle important pour assurer la défense de l'intérêt collectif des personnes fichées, dans le cas où leur préjudice n'est pas considéré comme suffisant pour leur assurer un accès à une réparation individuelle.

De même, un mécanisme d'action collective, ou *class action* (aggrégation d'intérêts individuels) peut faciliterer l'accès à une réparation judiciaire d'un préjudice subi par les personnes concernées, entre autre grâce à la simplification de la procédure, et à la diminution des coûts qu'il entraîne.

Notons, que, pour ces deux types d'actions, il importera de voir non seulement si elles existent dans le pays tiers, mais encore à quels domaines elles sont éventuellement limitées, si elles sont accessibles aux personnes qui ne sont pas citoyennes de ce pays,...

En conclusion, il apparaît important de mesurer, au regard d'un marché et d'une société déterminée:

1. le *degré de crainte* d'un responsable des traitements par rapport à une sanction en tenant compte de sa nature, de ses effets et de la qualité de l'autorité qui le prononce ;

2. l'*adéquation des sanctions* à la garantie du respect des principes de protection des données ;

3. *l'accessibilité des sanctions* (cfr. première et deuxième réflexions) ;

4. la qualité d'indépendance de l'organe qui prononce les sanctions et qui suppose que celui-ci ne se confonde pas avec une représentation des seuls intérêts des responsables de traitements.

CONCLUSION

L'analyse des moyens d'expression, de contrôle et de sanctions atteste d'une diversité très grande des solutions susceptibles d'être retenues pour arriver au résultat, à savoir le respect des principes essentiels.

Quelques conclusions peuvent cependant être tirées en ce qui précède:

1) chaque moyen doit être analysé dans se logique propre *et* en fonction du contexte du système juridique dans lequel il apparaît.

2) Chaque moyen renvoie à des conditions d'effectivité propres dont l'existence devra être établie.

3) Le résultat à atteindre dépend non d'un seul moyen mais toujours d'une combinaison de moyens d'expression, de contrôle, de recours et de sanction.

4) La combinaison de moyens proposées doit nécessairement garantir le respect non d'un seul principe mais de l'ensemble des principes, en particulier les deux principes essentiels: ceux de la participation individuelle et de la finalité.

5) Ces deux principes peuvent in concreto être consacrés par des moyens différents: ainsi, on peut imaginer vis-à-vis de traitements de l'Administration que le principe de participation individuelle fasse l'objet d'une consécration légale dans le cadre par exemple d'une loi d'accès aux documents administratifs, mais que le principe de finalité ne soit exprimé que par une charte, sorte de *privacy policy*, des administrations.

6) De manière générale, on peut considérer que plus faible est le moyen d'expression, plus il faudra être attentif à l'effectivité

des moyens de contrôle et de sanctions. On peut également affirmer que, sans exclure les autres, seront privilégiés des moyens qui permettent directement ou indirectement une action à partir de l'Union européenne. Ainsi notamment parmi les moyens de contrôle, le représentant, et parmi les moyens de sanctions, la sanction pénale qui permet la coopération policière.

7) L'effectivité des moyens de contrôle et de sanctions pour la personne européenne concernée suppose, en tout cas, la reconnaissance directe ou indirecte de droits d'accès et de contestation faciles à exercer et devant un organe indépendant du responsable du traitement. Chaque terme mérite à cet égard une explicitation:

- la reconnaissance des droits peut être directe ou indirecte: ainsi, en matière de codes de conduite, le droit pourrait être reconnu indirectement par le biais soit du contrat d'adhésion de l'entreprise responsable du traitement à ce code de conduite, ou par la reconnaissance judiciaire de ce code comme "règles de l'art".

- Si la notion d'accès a déjà été définie plus haut, la notion de contestation doit être entendue largement, c'est-à-dire au sens des différents principes de fond. Par "contestation", on entend non seulement la possibilité de mettre en cause l'exactitude d'une donnée (principe de qualité) mais également celle d'en contester la pertinence (principe de proportionnalité) voire, à l'occasion, plus fondamentalement la légitimité du traitement (principe de finalité).

A ce propos, on notera que certains des instruments internationaux déjà analysés ne consacrent le droit de contestation que de manière partielle, à propos du seul principe de qualité.

- La facilité d'accès suppose la possibilité d'une identification aisée du responsable du traitement et sur demande de la

personne concernée, la communication gratuite ou moyennant une redevance modérée dans un délai raisonnable sous une forme intelligible par la personne concernée des finalités du traitement et des données la concernant.

- La facilité de contestation suppose que les procédures mises en place pour assurer cette contestation soient transparentes, puissent être portées à la connaissance de la personne concernée et que le coût de leur mise en œuvre soit abordable.

- Il est à noter sur ces deux points que l'existence d'une (ou d') autorité(s) indépendante(s) au sens fonctionnel du terme est une garantie précieuse dans la mesure où celle-ci peut être un relais facile à l'étranger pour les personnes concernées voire pour les autorités nationales de protection des données.

- La contestation doit pouvoir être tranchée par un organe indépendant du responsable du traitement. Ce point est essentiel. Il signifie que l'existance de recours ne peut être le seul responsable du traitement ou un organe sectoriel représentant le seul point de vue des responsables de traitement. Nous l'avons vu, de nombreuses solutions peuvent exister pour satisfaire à cette exigence minimale.

8) Dans le cadre de l'analyse de la protection offerte par le pays tiers, il convient de ne pas perdre de vue l'influence du coefficient "différence culturelle" dont on a expliqué l'importance dans le chapitre II de la présente étude. En effet, la "différence culturelle" est susceptible d'avoir une influence notable sur la manière dont le pays tiers répond aux risques détectés.

Ainsi, par exemple, elle peut concerner les points suivants:

- la notion de finalité légitime peut varier de manière significative, entraînant des différences dans la manière dont

le besoin de légitimité est perçu, et dont le contrôle de la légitimité est effectué en pratique.

- Un autre point important est la sensibilité de la population vis-à-vis des moyens d'expression des principes de la protection des données: une population conscientisée aux enjeux de la protection des données représente une force de pression sur les autorités et sur le secteur privé pour le respect de principes protecteurs. Notons que le niveau de sensibilisation varie d'un pays à l'autre, mais également d'une époque à l'autre. Par exemple, les rédaction et promulgation de la loi taiwanaise de protection des données n'ont guère recueilli d'intérêt auprès du public ou des administrations, mais vu ses implications pratiques fort contraignantes, il est vraisemblable que la sensibilité à cette matière grandisse au fur et à mesure de l'application de la loi, s'il y a réelle volonté de l'appliquer.

Un élément peut être d'une grande aide dans l'appréhension de la différence culturelle existant au niveau des principes de fond: l'adhésion éventuelle du pays tiers à certains instruments internationaux concernant la protection des données. On pense en particulier à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ainsi qu'aux Lignes Directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontières de données de caractères personnel, du 23 septembre 1980. Ces deux instruments n'ont pas la même force, et il convient (en particulier pour les Lignes Directrices) d'être attentif à la manière dont ils sont mis en application dans le pays tiers (sur une base volontaire, avec force obligatoire?...). Cependant, l'adhésion à ces textes, si elle ne reste pas purement formelle, indique que le pays tiers attache de l'importance à la protection de la vie privée, et en a une vision qui n'est pas trop éloignée de l'approche communautaire.

Chapitre IV. Méthodologie

INTRODUCTION

Le but ultime du travail entrepris pour cette étude, est de proposer un outil d'aide à la décision destiné aux personnes chargées de la décision concernant un flux transfrontière de données au départ de l'Europe.

Pour ce faire, on suggère de réaliser une analyse en deux temps: il s'agit tout d'abord de déterminer les caractéristiques d'un flux ou d'une catégorie de flux en termes de risques et de facteurs de risque (i), et ensuite de procéder à l'examen de l'adéquation de la protection offerte par le pays tiers (ii).

(i) Nous avons vu que certains facteurs avaient une influence sur certains risques, et nous proposons donc un tableau d'analyse permettant de recenser aisément les facteurs de risque présents dans un flux particulier, et de déterminer à quel risque il faudra être particulièrement attentif (la méthode sera expliquée plus en détail ci-dessous).

(ii) Une fois que l'on a déterminé le(s) type(s) de risques spécifiquement entraîné(s) par le transfert, il s'agit de rechercher comment le pays tiers couvre adéquatement ce(s) risque(s). On sait en effet qu'il faut toujours évaluer le niveau de protection du pays tiers par rapport aux caractéristiques d'un flux déterminé.

Le sens des termes mentionnés dans ce chapitre est largement détaillé dans la partie explicative (constituée par les chapitres II et III de la présente étude). Toutefois, le tableau est suivi d'une note en expliquant l'usage.

L'utilisateur disposera de la sorte d'un outil lui permettant de relever rapidement les éléments-clés pouvant l'aider à prendre la décision. Toutefois, on rappelle encore qu'il s'agit d'un outil d'*aide* à la décision, qui ne peut remplacer l'analyse de chaque cas.

A l'usage, il est vraisemblable que certaines constantes se dégagent de la pratique: tel type de flux réalisé vers tel secteur dans tel pays pourrait alors être plus systématiquement autorisé (ou refusé, ou soumis à certaines conditions,...). Cependant, dans un premier temps, on ne pourra faire l'économie de l'examen détaillé des flux en question, à l'aide de la méthodologie proposée.

SECTION 1. MÉTHODOLOGIE

La méthodologie d'évaluation proposée se décompose en trois étapes, développées en détail dans ce chapitre.

1. Collecte des informations nécessaires (1.A)

2. Analyse des risques entraînés par le flux (1.B)

3. Analyse de la protection offerte par le pays tiers (1.C)

1.A. Collecte des informations nécessaires

§ 1. Remarque introductive: la "check-list"

Il est nécessaire, préalablement à toute analyse, de collecter des informations, tant au sujet du transfert ou de la catégorie de transferts étudiés qu'au sujet de la protection que l'on peut trouver dans le pays tiers. A ce stade, il importe d'essayer d'obtenir une information pertinente mais "non orientée", brute.

On suggère pour la collecte des informations nécessaires l'emploi d'une check-list, qui est présentée en annexe de cette étude et doit permettre de rassembler toutes les informations pertinentes tant au sujet du flux considéré que de la protection offerte par le pays tiers. La check-list ne contient que des questions descriptives, devant permettre de cerner le contexte du flux ainsi que celui de la protection offerte au transfert étudié par le pays tiers. L'analyse des réponses obtenues se fera à un stade ultérieur. On retiendra des parties différentes de la check-list, en fonction des personnes ou instances susceptibles d'y répondre.

§ 2. Personnes ou instances susceptibles de fournir l'information

Nous estimons que les deux types de personnes ou instances visées sont pour une part l'émetteur du transfert, et pour une autre des spécialistes de la protection du pays tiers (autorités de protection des données, ministères, experts,...).

(i) L'émetteur du transfert est à même de répondre aux questions concernant le flux lui-même (destinataire, données contenues, réseau utilisé, etc...). En outre, si l'émetteur du transfert est lié au destinataire (société-mère et filiales, sociétés du même groupe, membre d'une même organisation caritative, médicale, politique,...), il disposera également sans doute de connaissances relatives à la protection offerte au flux, si cette protection est, fût-ce seulement en partie, mise en place par l'organisation ou la société en question. On pense ici aux instruments tels les codes de conduite, privacy policy,... dont la société émettrice connaît l'existence et le contenu s'ils sont communs aux différentes sociétés du groupe ou de l'association à travers le monde. Il appartiendra alors à la société émettrice de collecter auprès du destinataire tous les éléments qui lui seront nécessaires pour fournir une réponse complète.

Dès lors, on suggère d'utiliser les parties de la check-list adaptées aux deux hypothèses suivantes: émetteur avec/sans lien avec le destinataire.

(ii) L'obtention des informations concernant la protection offerte par le pays tiers en-dehors de l'hypothèse où émetteur et destinataires sont liés est plus délicate. En effet, la désignation des personnes ou instances pouvant donner ces informations est susceptible de poser problème. Dans les pays tiers où existe une autorité indépendante de protection des données, on peut imaginer lui confier cette tâche. Par contre, dans tous les autres, il importe de trouver des spécialistes en la matière (fonctionnaires, membres d'une université, voire avocats,...) qui soient suffisamment indépendants pour ne pas répondre de façon biaisée aux questions.

On l'a dit plus haut, une partie de cette difficulté peut être surmontée en formulant les questions de manière objective, sans demander d'analyse ni d'évaluation à ce stade. Néanmoins, il est clair que toutes les questions ne pourront être neutres: par exemple, il nous semble que les réponses aux questions portant sur l'organisation judiciaire d'un pays et l'accès à la justice comporteront toujours une part d'évaluation personnelle. Dès lors, il sera peut-être opportun de désigner un expert extérieur, ou encore plusieurs experts travaillant séparément.

(iii) Il est imaginable d'envisager une troisième possibilité: la collecte des informations sur le flux serait toujours faite auprès de l'émetteur du transfert, mais la collecte des informations concernant la protection offerte par le pays tiers, ainsi que son évaluation seraient effectuées par des organisations indépendantes spécialisées dans cette matière. Ces associations pourraient éventuellement être agréées par la Commission, et se chargeraient de proposer un *rating* pour certains pays ou plus précisément certains secteurs concernés,

un peu de la même manière que les agences de *rating* évaluant les sociétés ou Etats lors d'émissions obligataires[1].

Notons que, si la collecte des informations doit se faire en deux temps, ce n'est pas seulement parce que les personnes ou organismes sont plutôt qualifiées pour répondre à l'une ou l'autre partie du questionnaire, mais aussi parce que la recherche d'instruments de protection adéquats dans le pays tiers est orientée par ce que l'on aura trouvé dans la première. Si par exemple, le transfert concerne des données médicales, on pourra rechercher des instruments de protection propres au secteur médical. Le choix des personnes devant répondre au deuxième questionnaire pourrait alors se porter sur des spécialistes de ce secteur pour le pays considéré.

§ 3. Le coefficient pondérateur "différence culturelle"

Il nous semble que c'est à l'issue de la deuxième partie de la collecte des informations que ce coefficient doit être pris en compte, car il est sans doute mieux connu de spécialistes du pays tiers que de l'émetteur du flux.

Il s'agit, pour chaque élément relevé dans le transfert considéré et dans la protection du pays tiers, de souligner l'influence

---

1 Le système de *rating* auquel sont soumis les sociétés ou les Etats lors d'une émission obligataire présente avec le système d'évaluation proposé dans le contexte des flux transfrontières certaines ressemblances intéressantes. L'évaluation faite par l'agence de *rating* vise en effet des éléments propres à un contexte d'opérations financières (tels par exemple que les comptes de la société, sa politique d'investissement, le soutien dont elle jouit de la part de l'Etat, le "risque-devise" existant dans le pays en question), mais également des facteurs non-financiers tels que la prise de mesures de sécurité adéquates, ou encore, le "risque-pays" (corruption, stabilité politique,...), qui est à peu de choses près l'équivalent de ce que nous avons appelé la "différence culturelle", transposée dans le domaine financier.
Le classement obtenu va de AAA (risque en principe nul), qui est en général la cote des Etats membres de l'OCDE à devise forte, à D ("défaut", lorsque le risque est très élevé). La société ou l'Etat émetteur peut malgré une mauvaise évaluation parvenir à trouver preneur pour ses obligations, à condition de fournir des garanties supplémentaires appropriées aux risques qui ont entraîné une mauvaise évaluation, ce qui n'est pas sans rappeler l'article 26.2 de la directive (mesures contractuelles appropriées dans le cas où la protection du pays tiers est jugée inadéquate).

d'éléments propres au pays tiers susceptibles d'avoir une influence sur l'évaluation des dits éléments. Ainsi, la différence culturelle peut viser aussi bien l'appréhension de la notion de données sensibles que par exemple le crédit à accorder à une *privacy policy*. Notons que, très logiquement, ce coefficient concerne plutôt la façon dont le pays tiers répond aux risques que les risques eux-mêmes.

1.B. Analyse des risques

A l'issue de la collecte, les personnes chargées de la décision sur le flux devraient disposer de toutes les informations pertinentes, mais à l'état "brut" (sauf si la collecte et l'analyse ont été confiées à une "agence de *rating*"). Il conviendra dès lors de les trier et les analyser en suivant les tableaux proposés ci-dessous. On commencera par l'analyse des risques, car c'est en fonction des risques entraînés par un flux que l'on doit évaluer l'adéquation de la protection offerte par le pays tiers.

Nous proposons pour l'analyse des risques un tableau destiné à faciliter le tri et l'évaluation des informations obtenues. Au départ d'une information purement factuelle, il doit permettre de dégager quelles caractéristiques du flux sont à prendre en compte particulièrement pour déterminer le niveau de protection souhaité.

On présente ici tout d'abord le tableau lui-même, et ensuite son "mode d'emploi", ainsi que des explications concernant plus particulièrement certains éléments de ce tableau.

§ 1. Présentation du tableau

Le tableau proposé a pour but de mettre synthétiquement en évidence les facteurs de risque pouvant être relevés dans un flux ou une catégorie de flux, ainsi que les risques augmentés ou diminués par ces facteurs.

Le tableau présente en ordonnée les "facteurs d'influence", et en abscisse les "risques", ainsi que, de manière distincte les "observations". La manière de remplir le tableau est détaillée ci-dessous dans le "mode d'emploi". Pour ce qui est du contenu des différents "risques" et "facteurs d'influence" mentionnés dans le tableau, on renvoie aux notions qui ont été développées dans le chapitre II de la présente étude.

§ 2. Tableau d'analyse des risques

	Perte de contrôle	Réutilisation	Manque de proportionnalité	Inexactitude des données	Observations
Situation socio-politique		*			
Retard technologique	*	*			
Technologie avancée		*			
Collecte indirecte des données	*	*			
Sensibilité des données			*		
Nombre de renseignements transférés			*		
Nombre de personnes concernées	*				
Fréquence des flux		*		*	
Type de transfert utilisé	*	*			
Localisation du fichier central	*				
Liens entre acteurs	*				
Secteur d'activité du destinataire	*	*			
Cohérence dans les finalités	*	*			
Durée de conservation des données		*	*	*	
Détermination de la finalité	*	*			

§ 3. Utilisation du tableau

a) Introduction

Une fois les informations nécessaires obtenues, il appartient à la personne chargée de la décision au sujet du flux de mettre en relation cette information "brute" avec les catégories proposées dans le tableau. Ainsi, s'il ressort des réponses à la check-list que le transfert considéré est effectué d'une maison-mère européenne à sa filiale située dans un pays tiers, on remplira aisément les cases "liens entre acteurs", "localisation du fichier central", "secteur d'activité du destinataire". Les autres questions de la check-list permettront évidemment de la même manière de remplir les autres cases ("pays de destination", "sensibilité des données", etc...).

b) Colonnes des "risques"

Comme on l'a vu dans le chapitre II de la présente étude, la plupart des facteurs repris sont susceptibles de jouer dans les deux sens. Par exemple, le type de transfert utilisé est un facteur d'influence qui peut soit augmenter, soit diminuer les risques: un transfert par un réseau ouvert augmente considérablement le risque, alors qu'un réseau fermé le diminue notablement

Par contre, certains facteurs peuvent n'avoir d'impact que dans un sens, et être neutres dans l'autre. Par exemple, si le nombre élevé de renseignements transférés peut augmenter le risque de non proportionnalité des données, le fait de ne transférer qu'un petit nombre de données ne diminue pas ce risque de manière significative (on ne notera donc rien dans le tableau pour ce critère).

Dès lors, on suggère de remplacer lors du remplissage du tableau les signes "*", destinés simplement à montrer sur quels risques les facteurs ont une influence spéciale,

- par un signe "+" lorsque le risque est augmenté;

- par un signe "-" lorsque le risque est diminué;

- par aucune mention lorsque ce facteur est neutre.

c) Colonne des "observations"

La colonne "observations" a pour fonction de permettre d'ajouter sous forme synthétique des éléments difficilement représentables par un simple signe, mais nécessaires pour l'analyse. Il est évidemment indispensable de mentionner par exemple la présence de données sensibles dans le flux, ce qui apparaîtra dans le tableau. Mais il nous semble également pertinent de décrire leur contenu, afin d'en estimer le degré de sensibilité dans le contexte du flux. Une observation s'imposera aussi s'il s'agit de données qui sont sensibles par leur contexte, tout en étant d'apparence anodine.

Un autre cas encore dans lequel l'emploi de la colonne "observations" se justifie pleinement est celui où la réalisation d'un risque est susceptible d'entraîner un dommage particulièrement important pour les personnes concernées. Une mention dans la colonne "observations" rappellera alors que même si les facteurs de risques paraissent peu nombreux, il faut entourer ce transfert de précautions particulières afin d'éviter la réalisation de ce risque.

Enfin, la colonne "observations" doit permettre de mentionner les incertitudes subsistant éventuellement quant à l'un ou l'autre élément du tableau (par exemple, quel est exactement le nombre d'éléments transférés, ou la fréquence des flux? Il est possible que l'information recueillie soit insuffisante pour déterminer si les facteurs en question sont suffisamment importants pour avoir une action sur les risques).

En résumé, les "observations" doivent permettre de disposer d'une vue plus complète du flux et d'affiner encore l'analyse qui en est faite.

§ 4. Remarques particulières

a) Données sensibles

On souligne la particularité du facteur "données sensibles". Il augmente sans doute le risque de manque de proportionnalité, comme on l'a expliqué dans le chapitre II, mais en outre, on ne peut négliger son action particulière sur les autres risques. En effet, si la présence de données sensibles dans un transfert n'augmente pas par elle-même la probabilité de réalisation du risque, elle en aggrave notablement les conséquences. La perte de contrôle sur des données médicales, par exemple, ou leur réutilisation, sont susceptibles de créer un dommage important. On suggère dès lors d'utiliser la colonne "observations" afin de mettre en évidence cette aggravation possible du dommage.

b) Evolutivité du tableau

Il est clair que ce tableau se veut être un outil évolutif et adaptable: si par exemple, lors de l'analyse d'un flux ou d'une catégorie de flux, un facteur de risque original se présente, on peut compléter le tableau, qui offre plutôt une méthode d'analyse qu'un cadre figé une fois pour toutes.

La même remarque vaut d'ailleurs pour l'analyse des moyens d'effectivité de la protection offerte par le pays tiers: s'il apparaît à l'expérience qu'une combinaison de moyens inédite offre une protection remarquable à certains types de flux, on pourra introduire cette combinaison dans l'analyse.

§ 5. Décisions possibles à l'issue de l'analyse des risques

Il est envisageable qu'avant même de passer à l'analyse de la protection offerte par le pays tiers, certains résultats apparaissent. Le résultat de l'analyse des risques peut conduire directement à deux types de conséquences portant soit sur le flux lui-même (a), soit sur la protection offerte par le pays tiers (b).

a) Conséquences au niveau du flux

(i) S'il ressort de la grille d'analyse des risques que le transfert considéré n'entraîne un risque (par exemple, manque de proportionnalité) qu'à cause de la présence d'un seul facteur de risque (par exemple, durée illimitée du traitement envisagé), alors que tous les autres paramètres conduisent à une évaluation positive, il peut être souhaitable de proposer à l'émetteur du flux de prendre une mesure diminuant ou supprimant l'impact de ce facteur (dans l'exemple cité, introduire une limitation de durée). De la sorte, la "dangerosité" du flux est fort réduite.

(ii) Dans une autre hypothèse, on peut même imaginer que la simple analyse du flux conduise à son interdiction vers certains pays, sans même prendre en compte la protection éventuellement offerte par les pays en question. Cela pourrait être le cas lors de l'envoi de données personnelles (par exemple, noms de journalistes travaillant pour des journaux ayant une couleur idéologique notoirement opposée à celle du pays en question) vers un pays soumis à un pouvoir dictatorial et non respectueux des droits de l'homme[2]. On peut également imaginer que la situation socio-politique d'un pays soit à ce point troublée (guerre civile) qu'il soit dangereux d'y transférer des données, quelle que soit leur nature.

Dès lors, dans un certain nombre de cas, l'analyse pourrait se limiter au flux lui-même, sans comporter d'évaluation de la protection du pays tiers.

b) Protection offerte par le pays tiers

Les résultats obtenus doivent également permettre de déterminer plus précisément quel degré de protection il est souhaitable d'obtenir dans le pays tiers. On relève deux "points de départ" possibles pour cette évaluation.

---

2 On pourrait peut-être imaginer d'autoriser le flux à condition d'anonymiser les données; cela reviendrait de toute manière à agir au niveau du flux, et non du pays tiers.

(i) Si le tableau d'analyse des risques fait ressortir que les risques d'inexactitude ou de manque de proportionnalité des données sont particulièrement élevés, on devra attacher une grande importance à la présence des principes protecteurs correspondants dans les moyens d'expression du pays tiers. On rappelle que le même raisonnement ne vaut pas pour les risques de perte de contrôle et de réutilisation, car les principes qui leurs correspondent sont considérés comme parties du "noyau dur" et doivent être dans tous les cas présents dans le pays tiers. Mais on peut imaginer d'être moins exigeant au sujet des principes d'exactitude et de proportionnalité si le risque ne paraît pas significatif.

(ii) Les facteurs d'influence relevés dans le tableau d'analyse des risques peuvent être efficacement pris en compte par différents moyens de contrôle (cette question sera reprise ci-dessous, dans l'analyse des moyens de contrôle). Par exemple,la localisation du fichier hors de l'Union européenne peut être contrebalancée par la nomination d'un représentant en Europe garantissant un accès effectif...

1.C. Analyse de la protection offerte par le pays tiers

Nous proposons pour cette partie de l'analyse une façon de procéder relativement différente de la partie consacrée aux risques. Il est en effet difficile de synthétiser en un tableau ou en une grille d'analyse le grand nombre d'éléments de natures différentes à prendre en compte dans l'analyse de la protection offerte par le pays tiers. La démarche suggérée se présente comme suit.

§ 1. Principes de fond

Il convient tout d'abord de déterminer quels principes de fond doivent être retrouvés dans le pays tiers. Les principes de participation individuelle et de légitimité faisant partie du noyau dur (voir à ce sujet le chapitre III de la présente étude), sont

fondamentaux et leur protection doit en tous les cas être assurée par le pays tiers.

Par contre, la nécessité de trouver dans le pays tiers la protection des principes de proportionnalité et de qualité des données est plutôt fonction des caractéristiques d'un transfert. Si l'analyse du flux démontre que les risques de non proportionnalité et d'inexactitude sont élevés, il faudra que ces risques soient couverts, outre la protection déjà assurée par les principes du "noyau dur".

§ 2. Moyens d'effectivité

Le chapitre III de la présente étude cernait un noyau dur de la protection des données, non seulement en termes de principes de fond, mais également en termes de moyens assurant l'effectivité de ces principes. Aussi, il convient, pour chacun des principes de fond recherchés dans le pays tiers, d'analyser les moyens qui assurent son effectivité. Pour ce faire, on recommande de confronter les informations recueillies grâce à la check-list au chapitre III, qui permet de déterminer si, au vu de ses caractéristiques, un moyen peut être pris en compte pour l'analyse.

a) Moyens d'expression et de sanction

(i) Il faut, pour chaque principe retenu, déterminer par quel moyen il est exprimé: code de conduite, norme établie par l'autorité publique, etc,... Notons que l'on peut très bien constater que les différents principes sont exprimés par des moyens différents (il faudra alors, à l'étape suivante, vérifier les moyens de contrôle de chacun d'entre eux).

Pour être retenu, chacun de ces moyens d'expression doit:

- être créateur de droits pour les personnes concernées (voir supra, chapitre III);

- s'appliquer aux étrangers non résidents sur le territoire du pays tiers (et en particulier, aux ressortissants de l'Union européenne);

- répondre aux conditions énoncées au chapitre III pour être pris en compte. Ainsi par exemple, une "privacy policy" doit être précise et complète, publique, et contrôlée dans son application.

Notons qu'en principe, l'analyse de la protection du pays tiers pourrait s'arrêter à ce stade-ci. Si un principe faisant partie du noyau dur ou jugé indispensable vu les caractéristiques du flux n'est pas exprimé (ou l'est seulement par un moyen jugé déficient à l'issue de l'analyse précitée), on sera amené à considérer le niveau de protection offert par le pays tiers comme inadéquat pour ce transfert.

(ii) Il faut ensuite voir à quels moyens de recours et de sanction le moyen d'expression renvoie: s'agit-il d'un moyen de recours particulier à ce moyen d'expression, ou renvoie-t-il plus généralement aux recours judiciaires? Ici aussi, il faudra pour chaque cas analyser l'effectivité des moyens de recours et de sanction, en tenant compte de ce qui en est dit dans le chapitre III. Chaque principe de fond doit être assorti de moyens de recours et de sanction qui lui sont propres. Cela implique qu'ici aussi, on pourrait considérer la protection du pays tiers comme inadéquate si aucune sanction appropriée n'est prévue pour l'un ou l'autre principe.

b) Moyens de contrôle

Chaque principe de fond retenu doit voir son effectivité assurée également par des moyens de contrôle. Les moyens de contrôle à rechercher sont, dans tous les cas, ceux qui font partie du "noyau dur de l'effectivité" tel qu'il est défini au chapitre III. Il s'agit des mesures de sécurité, de l'existence d'une autorité indépendante de contrôle, et de mesures garantissant l'accès des personnes concernées à leurs données.

L'analyse du flux permet de déterminer de façon plus précise quel niveau d'exigence est souhaitable pour admettre ces moyens; elle permet également de déterminer si d'autres moyens de contrôle sont appropriés. Ainsi, si le flux analysé est un flux "marketing", l'accès des personnes concernées devra leur permettre non seulement de vérifier les données les concernant, mais encore de s'opposer (*opt out*) au traitement. Si le pays tiers est affecté d'un retard technologique important, il importe que les mesures de sécurité prises par le responsable du traitement tiennent compte de ce facteur[3].Si le risque de perte de contrôle est accentué par de nombreux facteurs propres essentiellement à l'éloignement et la difficulté d'atteindre le maître du fichier, la nomination d'un "représentant" sera sans doute nécessaire.

On le voit, il est difficile de dresser un tableau de toutes les combinaisons de moyens possibles: elles sont fonctions d'éléments propres au flux considéré, et sont également influencées par la "différence culturelle". Cependant, il est vraisemblable que la pratique permette de dégager plus systématiquement des moyens ou combinaisons de moyens particulièrement adaptés pour tel ou tel type de flux.

Rappelons qu'une fois les moyens de contrôle nécessaires déterminés, il faut encore confronter les moyens trouvés dans le pays tiers aux exigences énoncées au chapitre III de la présente étude pour chaque moyen de contrôle. On recommande donc de suivre "pas à pas" le chapitre III pour chaque moyen de contrôle (comme d'ailleurs pour les moyens d'expression et de sanction).

---

[3] L'exemple classique étant celui de pays où la distribution électrique est déficiente, ce qui impose aux entreprises de pourvoir à une source alternative d'énergie (générateurs,...) pour éviter qu'une coupure de courant intempestive ne cause de dommage.

1.D. Remarque finale

On l'a dit, le but principal poursuivi lors de l'élaboration de la méthodologie est de fournir une méthode d'analyse, et non un outil qui conduise mathématiquement à une décision. Le résultat que l'on vise à obtenir, est la mise en relation de deux outils: d'une part une description du flux qui mette en évidence les facteurs de risques présents et les risques courus, et d'autre part, une description de la protection du pays tiers recensant les différents éléments susceptibles de constituer une protection adéquate.

La section qui suit a pour but de montrer, à l'aide d'exemples, la manière d'utiliser en pratique la méthodologie.

SECTION 2. FLUX-TESTS

Les exemples qui suivent ont pour but de montrer pas à pas la démarche à suivre pour l'utilisation de la méthodologie. Pour ce faire, nous partirons d'exemples de base permettant de développer plusieurs variantes(différents pays tiers, moyens d'expression, de contrôle, etc...).

2.A. Transfert de données relatives à la gestion du personnel

§ 1. Présentation du cas

On se base ici (en le modifiant légèrement) sur un des exemples donnés dans l'introduction de la présente étude: il s'agit de la création par une société étrangère disposant de sièges en Europe, d'une banque de données relatives au personnel de cadre, où qu'il soit, et recensant des renseignements de tous ordres. L'objectif pour cette société est de pouvoir répondre facilement à des besoins internes de la compagnie comme celui de la constitution d'équipes de

prospection d'un nouveau marché, de la recherche de formateurs, voire de la création d'une équipe sportive,...

Ces données collectées à partir de multiples sources -formulaires ou interviews lors des candidatures, appréciation par des supérieurs hiérarchiques, participation à des cycles de formation- sont en l'occurrence assemblées et envoyées à partir de lieux divers (centres de formation, directions du personnel des différentes entités locales,...) aux services centraux de direction du personnel de la multinationale.

§ 2. Collecte des informations nécessaires à l'évaluation

Ici, l'émetteur et le destinataire sont liés, puisqu'il s'agit d'une part de filiales, et d'autre part, de la société-mère. On demandera donc à l'émetteur des renseignements à la fois sur le flux considéré et sur l'existence éventuelle au niveau de l'entreprise d'un code de conduite ou d'une *privacy policy*. Les autres questions (relatives à la protection offerte par le pays tiers, et à l'influence du coefficient "différence culturelle) seront posées à des spécialistes du pays tiers.

§ 3. Analyse du flux: variante 1

La société-mère est une société de pétrochimie implantée dans un pays d'Asie du Sud-Est (appelé ci-après "pays A).

a) Tableau des risques

Le tableau des risques pour ce flux se présente comme suit (il sera commenté ci-dessous).

	Perte de contrôle	*Réutilisation*	*Manque de proportionnalité*	*Inexactitude des données*	Observations
Situation socio-politique					
Retard technologique					
Technologie avancée					
Collecte indirecte des données	+	+			
Sensibilité des données					
Nombre de renseignements transférés					
Nombre de personnes concernées					
Fréquence des flux		-		-	
Type de transfert utilisé	-	-			
Localisation du fichier central	+				
Liens entre acteurs	-				
Secteur d'activité du destinataire	-	-			
Cohérence dans les finalités	-	-			
Durée de conservation des données			+	+	
Détermination de la finalité	-	-			

On le voit, peu de risques se posent à cause du pays de destination lui-même: la situation socio-politique y est stable, l'état de la technologie y est assez avancé (mais les croisements de fichiers n'y sont pas une habitude répandue. Cette information ressort de l'analyse de la "différence culturelle").

Le flux lui-même présente quelques facteurs aggravant le risque: le fait que les données n'ont pas toutes été collectées auprès des personnes concernées, la localisation de la société-mère, et donc du fichier central et de l'archivage des données hors de l'Union européenne, ainsi que l'indétermination de la durée d'utilisation et de conservation des données.

Par contre, d'autres éléments diminuent le risque: le réseau utilisé est un réseau fermé (lignes louées par l'entreprise) totalement sécurisé, les transferts sont fréquents (les données sont souvent mises à jour), il existe un lien organique entre les acteurs, le secteur d'activité du destinataire n'est pas notablement "dangereux" (sa raison sociale n'est pas le commerce de données, et, par hypothèse, la société n'est active que dans le secteur de la pétrochimie, et n'a donc pas d'intérêt à faire profiter des sociétés du groupe ayant d'autres activités des informations obtenues), et les finalités du traitement sont connues, déterminées, et cohérentes (gestion du personnel, besoins internes à la multinationale). Enfin, par hypothèse, ce transfert ne comprend pas de données sensibles (aucune donnée médicale concernant le personnel, par exemple).

Les facteurs propres à ces transferts et aggravant les risques sont donc relativement peu nombreux. Néanmoins, certains risques sont présents: perte de contrôle, car les données provenant de différentes sources sont utilisées, et il peut être difficile pour la personne concernée de garder une maîtrise sur l'image d'elle que peuvent donner toutes ces informations rassemblées et recoupées. Le risque de réutilisation est également présent: si aucune norme ne l'empêche, la société mère peut tirer un bénéfice certain de la vente des informations concernant ses employés, car, par hypothèse, ces informations peuvent donner un profil assez précis des personnes concernées. Enfin, l'indétermination de la durée de conservation des données aggrave les risques de manque de proportionnalité et d'inexactitude des données; toutefois, on pourrait estimer que ces risques sont pris en compte par la fréquence des mises à jour opérées par la société-mère (vu la fréquence des flux). Toutefois, dans la

mesure où la société-mère ne précise pas que les données seront effacées par exemple lorsqu'un employé quitte la société (c'est-à-dire lorsque les mises à jour ne seront plus possibles), les risques d'inexactitude et de manque de proportionnalité demeurent.

b) Mesures envisageables au niveau des facteurs de risque

Il est possible de proposer à la société émettrice de prendre des mesures de manière à diminuer un risque propre au flux, ce qui permet de ne pas considérer la présence du principe correspondant dans le pays tiers comme fondamentale. Les risques considérés sont, en l'occurrence, ceux de manque de proportionnalité et d'inexactitude des données, risques qui ne nous semblent provoqués que par l'indétermination de la durée de conservation des données par la société. Dès lors, en proposant à la société émettrice de ne transmettre les données personnelles à la société-mère qu'à condition de définir la durée de conservation de ces données, et de la limiter en tout cas à la période pendant laquelle elle est en mesure d'y faire les corrections et mises à jour nécessaires, les deux risques cités sont sérieusement limités.

§ 4. Analyse du flux: variante 2

La société-mère est une société minière implantée dans un pays d'Afrique centrale en proie à des troubles économiques et politiques importants, ayant entre autres pour conséquence la désorganisation du système judiciaire, une insécurité importante, et une corruption présente à tous les niveaux de la société.

Il paraît clair que dans ce cas, la simple accumulation de facteurs propres au pays tiers et aggravant le risque peut mener à un refus de transfert des données, sans qu'il faille prendre en considération d'autres informations relatives au flux, voire à l'existence d'instruments de protection de ce pays, car on ne voit de toute manière pas comment ils pourraient être effectifs.

§ 5. Analyse de la protection du pays tiers: variante 1

L'hypothèse reprise ici est celle qui a été développée ci-dessus comme "variante 1": la société-mère est une société de pétrochimie implantée dans un pays d'Asie du Sud-Est, que nous appellerons "pays A".

a) Principes de fond

Il ressort de l'analyse des risques que les principes dont il faut rechercher l'effectivité dans le pays A sont ceux de participation individuelle et de finalité (qui font de toute manière partie du noyau dur). Nous retenons ici l'hypothèse ou la société a accepté de limiter la durée de conservation des données (le principe de proportionnalité et de qualité des données ne doivent pas être recherchés).

b) Effectivité des principes de fond

(i) Moyens d'expression et de sanction

La collecte des informations a permis de trouver dans le pays A deux moyens d'expression qui peuvent être pertinents:

- un décret d'exécution d'une loi portant sur les relations de travail (ce décret d'exécution porte spécifiquement sur le traitement des données, qu'elles soient à caractère personnel ou qu'il s'agisse de données de recherche scientifique,...);

- un code de conduite édicté par le secteur des industries chimiques du pays.

Le décret a été pris par le Ministère de l'Industrie et est applicable à toutes les données traitées par les entreprises du pays, quel que soit leur contenu: le critère de rattachement est le lieu du traitement. Il protège donc bien les données personnelles concernant les Européens. Il prévoit des sanctions pénales en cas de défaillance du maître du fichier, et renvoie à une procédure simplifiée pour

l'obtention éventuelle de dommages et intérêts. Ce décret correspond donc aux conditions définies dans le chapitre III pour être pris en compte comme moyen d'expression.

Toutefois, on ne peut en rester là pour la recherche de moyens d'expression, car ce décret n'édicte des règles qu'en matière d'information des personnes concernées, de qualité et de proportionnalité des données (ces derniers principes ne doivent, par hypothèse, pas être retenus ici). Par contre, le décret ne contient pas de disposition en matière de légitimité des finalités de traitement des données, ni d'ailleurs en matière de flux transfrontières au départ du pays A.

Il convient d'examiner alors si le code de conduite, appliqué dans le secteur des industries chimiques du pays énonce le principe de finalité.

Hypothèse 1: le code de conduite ne traite pas de cette question. Dans ce cas, si l'on ne peut pas trouver d'autre moyen d'expression qui contienne ce principe, la protection nous paraît inadéquate. En effet, le principe de finalité est fondamental et fait partie du noyau dur. En outre, la question des flux transfrontières au départ du pays tiers n'est pas réglée, ce qui fait perdre son effectivité à l'ensemble du système de protection des données personnelles, même celle assurée par le décret.

On peut imaginer alors que les sociétés émettrice et réceptrice choisissent de régler cette question par contrat.

Hypothèse 2: le code de conduite contient le principe de finalité. Il convient alors d'examiner si le code de conduite peut être pris en compte comme moyen d'expression. Il est créateur de droits pour les personnes concernées car, dans le pays A, les codes de conduite doivent être approuvés officiellement par le ministère dont dépend l'entreprise ou le secteur qui l'édicte. Le code que nous examinons engage le responsable du traitement et peut être invoqué

devant les tribunaux. Il protège également les données personnelles concernant des ressortissants de l'Union européenne, car il vise, comme le décret, toutes les données traitées par l'entreprise, indépendamment de leur provenance et de leur type.

Le mode d'élaboration de ce code de conduite répond (par hypothèse) aux conditions d'effectivité définies pour ce moyen d'expression dans le chapitre III de la présente étude. Il n'a pas fait l'objet d'une décision unilatérale par les responsables de traitement, mais a impliqué des représentants des travailleurs, ainsi que des membres de l'administration (qui ont eu pour mission entre autres de vérifier la réelle participation de toutes les parties concernées à l'élaboration du code). Cette condition (participation des différentes parties concernées) est particulièrement importante dans ce cas-ci, puisque l'on recherche une expression correcte du principe de finalité: il est important que la définition des conditions de légitimité des finalités ne soit pas conçue unilatéralement par les seuls responsables de traitements. En outre, dans la mesure où ce code est appliqué dans l'ensemble des industries chimiques du pays, il ne représente pas un point de vue minoritaire. Enfin, l'existence de ce code est connue, et l'entreprise a pour pratique d'en donner une copie à tous ses employés lors de leur engagement.

Le code de conduite envisagé renvoie à des sanctions de type civil: les personnes concernées peuvent s'en prévaloir de la même façon que si ses dispositions étaient incorporées à leur contrat de travail.

Enfin, il prévoit que les données traitées par l'entreprise ne peuvent être transférées à l'étranger qu'à la condition qu'elles bénéficient à l'étranger d'une protection identique à celles dont elles bénéficient dans le pays A.

Les moyens d'expression et de sanction répondent donc aux conditions pour constituer en partie une protection adéquate. Il reste à voir si les moyens de contrôle sont suffisants également.

(ii) Moyens de contrôle

Il faudra rechercher ici les moyens d'effectivité de chaque principe de fond retenu: il faut que, pour chacun, le "noyau dur de l'effectivité" (voir *supra*) soit présent (mais il est possible que certains éléments de ce "noyau dur" soient communs aux deux principes).

Chaque moyen d'effectivité doit être examiné en fonction de ce que l'on en dit dans le chapitre III de la présente étude.

• Effectivité du principe de participation individuelle

Mesures de sécurité

La société A traitant, outre les données personnelles des employés, des données scientifiques et commerciales d'une importance économique vitale pour elle, le système informatique est extrêmement sécurisé, et les données sont protégées contre la destruction, l'altération et la divulgation à des tiers non autorisés par des moyens physiques (accès aux locaux uniquement grâce à des cartes magnétiques, ...) et techniques (accès aux données limité entre autres grâce à un système de mots de passe à une partie du personnel selon ses fonctions, système de back-ups centraux fréquents,...) très complets. Notons qu'une partie des mesures de sécurité (par exemple les questions d'accès du personnel aux données) est réglée par le code de conduite que l'on a examiné ci-dessus; le reste des mesures est pris volontairement par l'entreprise.

Autorité indépendante de contrôle

Dans le pays A, les entreprises sont soumises à des contrôles fréquents par les ministères dont elles dépendent. Ces contrôles ont pour objet non seulement des vérifications financières ou comptables, mais encore d'obtenir la preuve du respect de toutes les réglementations en vigueur dans le pays et concernant les dites

entreprises (entre autres, donc, le décret sur le traitement des données personnelles). Pourrait-on dès lors considérer les ministères comme autorités indépendantes de contrôle pour les entreprises qui en dépendent? Il faut, pour répondre à cette question, vérifier différents éléments:

- fonctions remplies par ces organes: les ministères ont dans le système du pays A, des fonctions de promotion et de respect des principes de fond énoncés par la loi. Ils vérifient en outre que l'accès aux données est aisé, et interviennent en cas de difficulté; les personnes concernées peuvent s'adresser à eux en cas de refus d'accès, de correction, ou d'effacement de la part du responsable du traitement. Les ministères ont alors un pouvoir d'injonction vis-à-vis des entreprises concernées. Ceci n'exclut d'ailleurs pas des recours judiciaires.

- Indépendance de ces organes: du point de vue de leur composition, les ministères peuvent être considérés comme indépendants des entreprises privées, à condition toutefois que l'Etat n'ait pas une participation importante dans les dites entreprises, auquel cas, l'entreprise et l'Etat seraient trop liés pour que les ministères satisfassent au requis d'indépendance. Dans le flux-test que nous examinons ici, ce n'est par hypothèse pas le cas.

Le fonctionnement des ministères n'est pas totalement transparent (pas de publication d'un rapport d'activités, par exemple), mais les décisions prises sont accessibles au public, et, après leur signification à la personne concernée, peuvent faire l'objet d'un recours soit devant les tribunaux administratifs, soit devant une autorité supervisant le travail des ministères. Dès lors, il nous semble que le fonctionnement est suffisamment transparent; en outre, les ministères jouissent de considérables pouvoirs d'investigation, sur plainte ou d'initiative, ce qui leur assure un certain degré d'indépendance par rapport aux responsables de traitement qu'ils contrôlent.

- Accessibilité: les ministères sont facilement accessibles, et leur existence est forcément connue du public. Le seul problème pour les personnes concernées, peut être de savoir de quel ministère dépend l'entreprise qui traite leurs données, mais il existe un système de renvoi entre ministères.

La saisine est gratuite, et les ministères sont tenus de répondre aux demandes dans un délai déterminé.

- Effectivité des mesures prises par ces ministères: tant les moyens d'investigation des ministères que leurs moyens de contrainte vis-à-vis des entreprises, sont importants. Les sanctions qui peuvent être prises à l'égard de responsables de traitements défaillants sont fort lourdes (amendes, retrait de licence,...).

Il nous semble donc que, dans le cas analysé, le ministère titulaire de la société-mère située dans le pays A peut jouer le rôle d'autorité indépendante de contrôle (sans être créé sur le modèle occidental). Notons que le coefficient "différence culturelle" intervient dans cette évaluation: dans le pays A, l'administration a un rôle très actif, et respecté. Une entreprise qui aurait fait l'objet d'une sanction de la part de son ministère de contrôle souffrirait d'une très mauvaise publicité, que ce soit auprès du public ou dans son secteur d'activité. Ceci renforce l'effectivité de ce moyen de contrôle.

Accès de la personne concernée

En matière d'accès et d'information de la personne concernée, on note deux types de mesures: les unes sont imposées par le décret, et les autres sont prises sur initiative de la société-mère.

Le décret fait peser sur le responsable du traitement une série d'obligations en matière d'information de la personne concernée; en outre, les ministères de contrôle doivent vérifier le respect de ces

obligations, et pouvaient intervenir pour en exiger l'application de mesures appropriées.

Une information très complète doit être donnée à la personne concernée lors de la collecte (ce qui ne nous concerne pas ici, puisque, par hypothèse, la collecte a été effectuée en Europe), ou lors d'un changement de finalité de traitement, ou, de toute manière, une fois par an. Cette information porte aussi bien sur les données détenues par le responsable que sur les finalités du traitement, ainsi que les modalités d'accès, ou les possibilités de rectification ou de radiation de certaines données.

L'entreprise que nous examinons a mis en place, outre ce système d'information légalement obligatoire, un système supplémentaire pour les membres de son personnel localisés à l'étranger (sur le territoire de l'Union européenne, par exemple). Elle a prévu dans ce cas que l'information pouvait se faire sur demande: cette demande doit être communiquée à un service responsable institué dans sa plus importante filiale européenne, située à Manchester. Notons qu'il ne s'agit pas de la formule du "représentant" dont il est question dans le chapitre III de la présente étude, car le service en question n'a pas pour fonction de veiller au respect du prescrit de la directive; il doit simplement jouer un rôle d'intermédiaire entre la maison-mère et les filiales pour tout ce qui concerne la gestion du personnel. Toutefois, son existence facilite considérablement l'accès des personnes concernées aux données et renforce l'impact de ce moyen de contrôle.

A ce stade, on le voit, le noyau dur des moyens d'effectivité est présent pour le principe de participation individuelle. On pourrait, nous semble-t-il s'arrêter ici dans l'analyse des moyens d'effectivité, et considérer la protection du pays A comme adéquate pour ce principe: le flux présentant un nombre peu élevé de facteurs de risque, et l'efficacité des trois moyens de contrôle existants sont

des facteurs positifs. En outre, la présence officielle d'un relais européen, même s'il ne peut être considéré comme un "représentant" est également un point important.

Toutefois, on note qu'il existe encore dans le pays A un autre moyen de contrôle: un système de notification préventive auprès des ministères responsables. La notification doit être réitérée à chaque changement d'éléments importants du traitement: finalité, données concernées,... Sur base de ces notifications, les autorités de contrôle peuvent prendre diverses mesures préventives, comme par exemple, négocier avec l'entreprise concernée une meilleure information du public, ou la prise de mesures de sécurité adéquates.

• Moyens de contrôle du principe de finalité

Il s'agit du principe qui était exprimé dans le code de conduite. Notons que certains moyens de contrôle peuvent être communs avec ceux que nous venons de mentionner pour les principes énoncés dans le décret. Ainsi, les mesures de sécurité prises par l'entreprise assurent l'effectivité du principe de légitimité des finalités aussi bien que des autres principes cités plus haut. En ce qui concerne les autres moyens de contrôle, il convient également de voir s'ils assurent l'effectivité du principe de finalité. Ainsi, par exemple, l'autorité indépendante de contrôle peut être identique, mais il faut vérifier si ses pouvoirs d'investigation, de sanction, etc,... portent également sur le principe de finalité.

Autorité indépendante de contrôle

Dans le pays A, on l'a dit, l'application des codes de conduite est supervisée par les ministères. On renvoie à l'examen qui en a été fait ci-dessus et tendait à montrer que ces ministères répondent aux conditions fonctionnelles pour être considérés comme des autorités indépendantes de contrôle. Dans la mesure où leurs tâches de contrôle portent également sur le contenu des codes de conduite, on peut considérer que ce moyen de contrôle est rempli ici aussi.

Notons qu'on aurait pu concevoir qu'il existe une autre autorité indépendante de contrôle pour ce principe, comme par exemple, une commission sectorielle mise en place par le code de conduite. Il aurait fallu dans ce cas analyser cette commission de façon à voir si elle pouvait être considérée comme autorité indépendante.

Accès

On a déjà détaillé précédemment les mesures prises par le responsable du traitement pour assurer l'accès des personnes concernées aux données. Il convient donc d'examiner ici si cet accès permet aux personnes concernées une vérification, voire une contestation de la légitimité du traitement, et, en outre, si l'autorité indépendante de contrôle peut les aider dans ces démarches, en cas de problème ou de contestation. Dans ce cas-ci, le code de conduite renvoie à l'action de ces ministères qui peuvent assurer le respect du code de conduite comme s'il s'agissait d'une norme issue de l'autorité publique.

§ 6. Conclusion de l'analyse de ce flux-test

Le noyau dur est présent dans le pays tiers, tant au niveau des principes de fond que de leur effectivité (expression, contrôle et sanction). Des recours sont accessibles aux personnes concernées en cas de défaillance, que ce soit à un niveau interne à l'entreprise (par l'intermédiaire du relais installé en Europe), à un niveau administratif (autorité indépendante de contrôle) ou à un niveau judiciaire (procédures devant les tribunaux). A cet égard, on relève l'existence de sanctions pénales, ce qui permet éventuellement à la personne concernée de s'appuyer sur la coopération entre polices en cas d'infraction au décret.

Il nous semble donc que le transfert effectué dans ces conditions peut être autorisé.

2.B. Transfert de données marketing

§ 1. Présentation du cas

Une entreprise belge de sondages marketing collecte les données principalement auprès des personnes concernées à partir d'un vaste questionnaire portant sur les habitudes de consommation (voyages, alimentation, culture,...). Elle vend les données obtenues à une société sise dans un pays tiers qui exécute les tâches d'encodage, de triage, voire de sélection. Les données sont transférées sur un support papier. Après leur encodage dans le pays tiers, ces données sont croisées avec d'autres données: numéro de téléphone, importance de la localité, type de quartier (revenu moyen par habitant, etc...) provenant de sources publiques accessibles directement de l'étranger ou transférées par support informatique. Une fois triées, ces listes sont revendues à différents clients désireux de commercialiser certains produits sur le marché belge auprès d'un public ciblé.

§ 2. Collecte des informations nécessaires à l'évaluation

Les informations concernant le flux seront demandées à l'émetteur (la société belge). Dans la mesure où les sociétés émettrice et réceptrice ne sont pas organiquement liées, toutes les informations concernant le pays tiers devront être demandées à des experts en la matière.

§ 3. Analyse du flux et de la protection du pays tiers

Le pays tiers est un pays d'Europe de l'Est à l'industrie très peu développée, et au retard technologique important.

a) Analyse des risques

(i) Le tableau des risques se présente comme suit:

	Perte de contrôle	*Réutilisation*	*Manque de proportionnalité*	*Inexactitude des données*	Observations
Situation socio-politique					
Retard technologique	+	+			
Technologie avancée					
Collecte indirecte des données					(1)
Sensibilité des données					(2)
Nombre de renseignements transférés			+		
Nombre de personnes concernées					
Fréquence des flux					
Type de transfert utilisé	+	+			
Localisation du fichier central	+				
Liens entre acteurs	+				
Secteur d'activité du destinataire	+	+			
Cohérence dans les finalités					
Durée de conservation des données					
Détermination de la finalité					

Observations:

- Observation (1): la collecte d'une partie des données a été faite directement auprès des personnes concernées, mais cet élément ne nous paraît pas être de nature à diminuer le risque car les données sont destinées à être croisées avec des données provenant d'autres sources.

- Observation (2): le transfert ne comporte pas de données sensibles comme telles. Cependant, le recoupement d'informations relatives au nom, au domicile, et à certaines habitudes de consommation peut permettre l'obtention de données relatives à la race ou à la religion. Lors de l'analyse de la différence culturelle, il conviendra d'être attentif à cet élément, et de voir en particulier ce que le pays tiers risque d'en faire

(ii) Analyse du tableau

Le tableau fait apparaître un nombre important de facteurs aggravant les risques. Le pays tiers est par hypothèse affecté d'un important retard technologique, ce qui rend difficile la prise de mesures de sécurité adéquates. Le nombre de renseignements transférés est considérable et porte sur une grande variété d'éléments. Le type de transfert (support papier) est susceptible d'aggraver les risques dans la mesure où un document imprimé nous paraît relativement facile à reproduire et détourner même dans un pays où la technologie informatique n'est pas moderne. Le fichier central est localisé dans le pays tiers de façon permanente; il n'y a pas de lien organique entre les acteurs; en outre, le secteur d'activité du destinataire (courtage en données) aggrave aussi considérablement les risques, puisque cette activité consiste à croiser et vendre des données. Notons que, dans notre hypothèse, la conservation des données est limitée dans le temps (cela correspond à l'intérêt économique du responsable du traitement, car ces données se périment très vite).

Les risques de perte de contrôle et de réutilisation sont donc importants, et les conséquences de la réalisation de ces risques pourraient être alourdies par la déduction possible d'éléments tels la race ou la religion à partir du croisement de données du flux avec d'autres données. Le risque de manque de proportionnalité existe également: il est induit à la fois par le nombre de renseignements transférés et par le croisement de ces renseignements avec d'autres.

b) Analyse de la protection du pays tiers

Il ressort de l'analyse du flux que les principes de participation individuelle, de finalité, et de proportionnalité doivent être présents dans le pays tiers.

(i) Moyens d'expression et de sanction

Dans le pays B, il existe une législation générale de protection des données à caractère personnel, adoptée récemment, et inspirée entre autres de la Convention 108 du Conseil de l'Europe. Cette législation reprend les trois principes mentionnées ci-dessus. Elle a été prise au niveau fédéral, et s'impose à tous les traitements qui ont lieu dans le pays. Il est difficile de savoir si elle s'applique ou non aux étrangers non résidents dans le pays B; il n'existe aucune jurisprudence sur le sujet, mais la Constitution n'affirme pas le contraire de manière claire. On peut donc considérer avec un degré raisonnable de certitude que des étrangers pourraient l'invoquer, d'autant qu'elle vise les traitements, sans mentionner la provenance des données qui en font l'objet.

Cette législation prévoit des sanctions civiles, mais l'organisation judiciaire du pays B présente certaines déficiences graves (complexité de la saisine des tribunaux et longueur des procédures essentiellement). Ceci représente un facteur négatif, qui doit appeler l'attention sur l'existence éventuelle de recours extra-judiciaires, éventuellement auprès d'une autorité de contrôle.

(ii) Moyens de contrôle

Mesures de sécurité

Considérant les facteurs de risque présents dans ce flux, il convient d'être particulièrement exigeant au sujet des mesures de sécurité prises dans le pays tiers. Vu le retard technologique qui y existe, et les risques inhérents à un transfert sur support papier

(impossibilité de cryptage des données,...), il faut que la société destinataire compense cela par la prise de mesures de sécurité très complètes. Or, par hypothèse, les mesures de sécurité prises par l'entreprise destinataire sont très insuffisantes. L'accès aux locaux n'est pas contrôlé; il n'existe pas de système de back-up régulier, le local où se trouvent les imprimantes utilisées pour la publication des listes est partagé par une autre société totalement indépendante,...

§ 4. Conclusion de l'analyse de ce flux

Il nous semble que, vu la gravité des lacunes dans l'effectivité de la protection au regard des risques entraînés par le flux en question, ce dernier ne peut être autorisé. Même si la législation énonce de manière précise et détaillée l'ensemble des principes de fond, leur effectivité ne peut être assurée dans les conditions décrites ci-dessus.

Notons que, si l'on avait pu poursuivre cette analyse, il aurait fallu vérifier la possibilité de recours extra-judiciaires (vu la déficience du système judiciaire), ainsi que la possibilité pour les personnes concernées de s'opposer au traitement (car il s'agit d'un traitement "marketing").

Conclusion

Il s'agit ici de synthétiser les principaux apports de la présente étude.

1. La notion de "protection adéquate", condition mise au flux de données personnelles vers des pays extérieurs à l'Union européenne se caractérise comme suit: sans exclure une analyse plus globale de la situation d'un pays tiers, elle suppose au sens de l'article 25 alinéa 2:

- une approche au cas par cas, c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée par rapport à un flux ou une catégorie de flux. L'instrument méthodologique doit caractériser de manière précise le cas visé;

- une approche souple et ouverte puisque selon le libellé même de l'article 25 § 2 l'évaluation doit pouvoir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque Etat, voire chaque responsable des données, peut apporter, l'article 25 § 2 étant purement indicatif à ce propos. L'instrument méthodologique doit refléter cette ouverture et cette souplesse, et être adaptable aux multiples cas rencontrés ou à rencontrer;

- une approche fonctionnelle, c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place

par le responsable des données dans le pays tiers pour pallier ces risques.

L'évaluation de ces mesures doit se faire sans a priori; il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d'impérialisme européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ par la directive; au contraire elle crée pour l'évaluateur la nécessité de prendre en considération les adaptations originales des modalités de cette protection, ceci tout en maintenant les exigences qui fondent selon la directive le besoin de protection. L'instrument méthodologique doit laisser la place à cette variabilité de nature et de portée des solutions apportées.

2. Les caractéristiques de l'approche ci-dessus mentionnées, conduisent à distinguer diverses notions, dont la méthodologie d'analyse du flux devra tenir compte.

2.1. Ainsi, la protection n'est jamais adéquate que si elle est la réponse appropriée aux risques d'un flux, c'est à des événements dont la probabilité de survenance lors d'un flux dépend d'un certain nombre de facteurs et qui entraîne pour la personne fichée un dommage.

Quatre risques essentiels sont identifiés: la perte de contrôle, la réutilisation des données, le manque de proportionnalité et l'inexactitude des informations.

Nombre de facteurs doivent être pris en compte; certains sont propres à la dimension transfrontière du flux, d'autres interviennent dans l'appréciation de n'importe quel flux. Il importe de les isoler et

d'analyser à chaque fois leur portée par rapport aux risques envisagés.

Quant aux dommages peuvent être immatériels, matériels ou même constituer une atteinte à la sécurité ou l'intégrité physique des personnes

2.2. Pour constitier une réponse appropriée, la protection doit garantir le respect des principes de fond (2.2.1.) de la protection des données de manière effective (2.2.2.)

2.2.1. Les principes de fond constituent donc les objectifs de la protection, le référent de celle-ci, dont le respect doit être assuré. Ces principes se déduisent tant de l'analyse des risques que du contenu de tous les instruments existants de protection des données.

Leur existence se fonde sur la volonté essentielle de tout instrument de protection des données d'assurer à l'individu une maîtrise de la circulation de son image informationnelle et de son utilisation (principes de participation individuelle et de finalité) et sur leur volonté accessoire de permettre un contrôle des caractéristiques de cette image informationnelle dans sa qualité (principe de qualité) et son ampleur (principe de proportionnalité).

Par rapport à certains de ces instruments la directive se distingue en ce sens:

- qu'en exigeant une finalité "légitime", elle introduit l'idée d'un certain contrôle social de justification de l'utilisation de cette image informationnelle, en d'autres termes, qu'elle n'abandonne pas à la seule discrétion du responsable du traitement, la définition des finalités.

- Que par l'exigence de consentement ou par l'ouverture de possibilités d'opposition, elle entend accroître la maîtrise de l'individu sur l'utilisation de son image informationnelle, chaque fois que la légitimation du traitement est délicate soit en raison de la nature des données, soit en raison de l'absence de relation contractuelle ou réglementaire préalable entre la personne concernée et le responsable du traitement.

2.2.2. L'effectivité du respect des principes se déduit de l'examen d'une pluralité de techniques, premièrement d'expression de ces principes, deuxièmement de contrôle et de mise en œuvre de ces principes, et troisièmement de recours ou de sanctions prévues en cas de non respect de ces principes. Si de multiples combinaisons de ces techniques, catégories par catégories et entre catégories sont possibles, il est possible cependant de définir un noyau dur:

- à propos des techniques d'expression, peu importe celles choisies, qu'elles confèrent à la personne concernée un droit susceptible d'être revendiqué devant un tribunal. Ce droit est nécessaire si on souhaite que l'effectivité des principes ne soit pas laissée à la discrétion des responsables de traitement.

- A propos des techniques de contrôle et de mise en œuvre, trois techniques semblent s'imposer:

(i) les mesures de sécurité internes et le cas échéant externes (réseaux de télécommunications) dans la mesure où sans elles les garanties offertes par les autres moyens risquent de rester lettre morte.

(ii) L'accès de la personne concernée, dans la mesure où il représente le moyen le plus évident de réalisation du principe de participation individuelle et en même temps la

meilleure technique de contrôle du respect des autres principes.

(iii) L'autorité indépendante de contrôle prise non au sens institutionnel de la directive mais bien fonctionnel c'est-à-dire assurant un certain nombre de missions, peu importent la forme et le statut concret de cet organe. L'existence de cet organe se justifie à la fois par la volonté de rendre effectifs les deux principes majeurs de la protection des données. Le premier réside en ce que la participation individuelle nécessite un organe relais en particulier dans le cadre de flux transfrontières et implique un droit de ne pas être laissé seul; le second principe est que le contrôle "social" des finalités d'utilisation suppose la possibilité de débats publics devant des instances neutres ou en tout des initiés par elles.

- Enfin, à propos des techniques de recours et de sanctions, peu importe leur nature, elles doivent assurer le droit à une procédure contradictoire d'accès aisé. Le moyen de sanction doit être en relation avec la (ou les) technique(s) d'expression choisi(s).

3. La méthode d'analyse des flux et de la protection adéquate au regard de ces flux se déduit des caractéristiques de la notion de protection "adéquate", des distinctions proposées et des éléments du "noyau dur" retenus. L'étude l'applique à quelques cas concrets.

3.1. La première question est préjudicielle : quelles informations collecter? Un questionnaire permet dans un premier temps d'identifier les caractéristiques des flux, dans un second temps, de collecter l'information nécessaire sur les techniques de protection existant dans le pays tiers où est localisé le destinataire du

flux (techniques d'expression, de contrôle, de recours et de sanctions).

Il va de soi que c'est auprès du responsable du traitement émetteur du flux et localisé en Europe que s'opérera la collecte d'informations sur le flux lui-même; exceptionnellement elle pourra être opérée auprès du responsable localisé hors Europe si l'information est directement recueillie par lui auprès de la personne concernée (cas de collecte via Internet, par exemple). La collecte des informations sur la protection offerte par le pays tiers se fera auprès de spécialistes, d'experts de ce système de protection.

3.2. La seconde question est plus épineuse: qui analyse les données issues du questionnaire? Si la décision finale est du ressort des autorités nationales ou communautaires, on peut imaginer que cette décision s'appuie sur l'analyse préalable d'experts voire que cette expertise soit construite sur le modèle du "rating" déjà existant dans le domaine des risques financiers à l'exportation. Cela permettrait en particulier une meilleure prise en considération du coefficient "différence culturelle". Ce coefficient joue tant dans l'appréciation des facteurs de risques (ex. habitude des sociétés de marketing de s'échanger les fichiers; conception différente de la sensibilité des données, ...) que dans l'évaluation de l'effectivité des techniques de protection (ex: valeur juridique d'une privacy policy, neutralité d'une autorité sectorielle de contrôle, ...). La prise en considération de ce facteur répond à la volonté des auteurs de la directive de ne pas imposer leur modèle et nécessite une expertise du système sociétaire étranger.

3.3. Enfin, la troisième question a trait à la décision. Nous proposons deux étapes à celle-ci.

La première se déduit de l'analyse des facteurs: des risques il est sans doute possible de jouer sur l'un ou l'autre facteur afin de réduire le risque. Suivant les facteurs, l'attention sera portée sur la

mise en cause de tel ou tel principe de fond dont la vérification du respect devra alors faire l'objet d'une attention particulière.

La seconde analyse l'adéquation des combinaisons de moyens proposés en deux temps. Pour chaque moyen proposé, doit avoir lieu une vérification des conditions propres d'efficacité. Il peut alors être procédé à la seconde phase: la combinaison de moyens permet-elle de répondre aux exigences posées par le noyau dur de la protection et ce pour les principes mis en cause, en toute hypothèse pour les deux principes majeurs.

Principales références bibliographiques

ARETE, *Les réseaux informatiques internationaux et la protection des données personnelles*, Etude pour la Commission des communautés européennes (DG XV), Mars 1995.

K. BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Thémis, Montréal, 1992.

K. BENYEKHLEF, La souveraineté nationale et le contrôle des échanges internationaux d'information, *La Revue Juridique Thémis,* 25, 1991, pp. 433 et suiv.

C.J. BENNETT, Canada Under the Gaze of the European Sphinx, *Privacy Files*, Vol.1, No 1, Oct. 1995, pp. 13 et suiv.

C. J. BENNETT, *Regulating privacy*, Ithaca, Cornell University press, 1992.

C. J. BENNETT, *Privacy codes, privacy standards and privacy laws: the instruments for data protection and what they can achieve*, Paper presented at visions for privacy conference in Victoria, British Colombia, 9-11 mai, 1996.

A. BOURLOND, Y. POULLET, Flux transfrontières de données à caractère personnel, position de la proposition de directive européenne face à celle de la convention 108 du Conseil de l'Europe, *Droit de l'informatique et des télécoms*, 1991/2, pp. 58 et suiv.

A. BRANSCOMB, Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition, *Vanderbilt Law Review*, Vol. 36:985, 1983, pp. 985 et suiv.

M. BRIAT, CH. PITRAT, Protection des données. Autoroutes électroniques et flux d'informations, *Droit de l'informatique et des télécoms*, 1994/3, pp. 6 et suiv.

U. BRÜHANN, *The US response to the European Union's Data Protection Directive*, Contribution made for the Conference "Managing Privacy in Cyberspace and Across National Borders", Washington, 10 October 1996.

P.A. COMEAU, A. OUIMET, Freedom of Information and Privacy: Québec's Innovative Role in North America, *Iowa Law Review*, March 1995, vol.80/N°3, pp. 651

W.J. DEARHAMMER, *Transborder Data Flow. Implication for Credit Information Exchange*, 1983, R.M.A., Philadelphia.

L. EARLY, Securing equivalent protection among nations in the context of transborder data flows: a possible role for contract law, *Droit de l'informatique et des télécoms*, 1990/4, pp. 10 et suiv.

O. ESTADELLA-YUSTE, The Draft Directive of the European Community regarding the Protection of Personal Data, *International and Comparative Law Quarterly*, 1992, Vol. 41, p. 170 et suiv.

D. FARNSWORTH, Data Privacy or Data Protection and Transborder or Transnational Data Flow, an American's View of European Legislation, *International Business Lawyer*, 1983, Vol. 11, pp. 171 et suiv.

D. FLAHERTY, *Protecting privacy in surveillance societies*, Chapel Hill, University of North Carolina Press, 1989.

L. HAECK, The protection of personal data used for the purposes of direct marketing and the IATA recommended practice

on transborder data flows, *Air Law*, vol. XIII, Nr 4/5, 1988, pp. 178 et suiv.

L. HAECK, Les flux transfrontières de données (de caractère personnel) et les lignes aériennes internationales, *Annales de Droit Aérien et Spatial*, Vol. VIII, 1983, pp. 85 et suiv.

R. LAPERRIÈRE, R. CÔTÉ, G.A. LEBEL, The transborder flow of personal data from Canada: international and comparative law issues, *Jurimetrics Journal*, Vol. 32, No. 4, 1992, pp. 547 à 569.

R. LAPERRIÈRE, R. CÔTÉ, G.A. LEBEL, *Vie privée sans frontière*, Ministère de la justice du Canada, 1990.

J. NOUWT, H.A.C.M. VORSELAARS, Privacy in Cyberspace, *Emerging electronic highways*, Kluwer law international, 1996, p. 103 a 120.

M. NUGENT, International Banking. Cross-Border Transmission of Financial Information: The Cyberbanking Concerns, *Banking Policy Report*, March 4-18, 1996, pp. 31 et suiv.

M. NUGENT, U.S. Business and the european data directive, *Privacy and American Business*, 1995

A.C.M. NUTGER, *Transborder Flow of Personal Data within the EC*, Deventer, Kluwer, 1990.

O. ORTNER, The Privacy Protection Aspect of Transborder Data Flow, *International Business Lawyer*, April 1984, pp. 171 et suiv.

CH. PITRAT, Clauses modèles pour les flux transfrontières de données, ou comment assurer une protection équivalente, *Droit de l'informatique et des télécoms*, 1993/1, pp. 46 à 52.

Y. POULLET, Privacy Protection and Transborder Data Flow; Recent Legal Issues, in *Advanced Topics of Law and Information Technology*, G.P.V. VANDENBERGHE (ed.), Kluwer, Deventer, 1989, pp. 29 et suiv.

Y. POULLET, The european directive relating to the protection of physical persons with regard to the processing of personnal data and its free circulation - a state of relative harmony, in *A business guide to changes in european data protection legislation*, Cullen International, nov. 1996.

J. REIDENBERG, Setting Standards for Fair Information Practice in the U.S. Private Sector, *Iowa Law Review*, March 1995, vol.80/N°3, pp. 497 à 551.

C. RUMBELOW, Privacy and Transborder Data Flow in the UK and Europe, *International Business Lawyer*, April 1984, pp. 153 et suiv.

N. SAVAGE, CH. EDWARDS, Transborder Data Flow: the European Convention and United Kingdom Legislation, *International and Comparative Law Quarterly*, 1986, Vol. 35, pp. 710 et suiv.

P. SCHWARTZ, European Data Protection Law and Restrictions on International Data Flow, *Iowa Law Review*, March 1995, vol.80/N°3, pp. 471 à 496.

P. SCHWARTZ, J. R. REIDENBERG, *Data privacy law; a study of United States data protection*, Charlottesville, Va., Michie, 1996.

S. SIMITIS, From the Market to the Polis: the EU Directive on the Protection of Personal Data, *Iowa Law Review*, March 1995, vol.80/N°3, pp.445 à 469.

D. SLEE, Privacy and the European Union: an examination of the provenance and content of the forthcoming Data Protection Directive and its likely impact on UK data protection law, Law, *Computers & Artificial Intelligence*, Vol.4, No. 3, 1995, pp. 277 à 297.

G. TRUBOW, The European Harmonization of Data Protection Laws Threatens U.S. Participation in Transborder Data Flow, *Northwestern Journal of International Law & Business*, 13:159, 1992, pp. 159 et suiv.

D. YARN, The Development of Canadian Law on Transborder Data Flow, *Georgia Journal of International and Comparative Law*, Vol. 13:825, 1983, pp. 825 et suiv.

La protection de la vie privée eu égard aux renseignements personnels détenus dans le secteur privé, Mémoire du Barreau du Québec, Août 1991, Montréal.

Annexe I

CHECK-LISTE

I. Description générale du flux

1. Responsable du traitement dans le pays d'origine

Coordonnées complètes du responsable du traitement dans le pays d'origine: nom et prénoms, ou dénomination de la société ou l'association, adresse, secteur d'activité, n° TVA le cas échéant,...

2. Destinataire du fichier dans le pays tiers

A. Coordonnées complètes du destinataire du fichier: pays et région, nom et prénoms ou dénomination de la société ou l'association, adresse, secteur d'activité, ...

B. Le fichier central est-il situé sur le territoire de l'Union Européenne ou dans le pays tiers?

C. Le destinataire est-il un individu ou une organisation directement liés à l'émetteur (autre société du même groupe, filiales, employé ou agent, fournisseurs de biens ou de services,...). Détailler.

D. Dans quelle catégorie d'activité se situe le destinataire:

1. Sociétés privées (Marketing, courtier en données, organisations politiques, associations ou organisations bénévoles, caritatives ou religieuses,...). Détaillez.

2. Services de santé (Mutuelles, hôpitaux, médecins, autres agents du secteur soins de santé,...). Détaillez.

3. Banques et compagnies d'assurances (Banques, compagnies d'assurances, agences d'évaluation de la solvabilité, agences de recouvrement de créances, autres organisations financières,...). Détaillez.

4. Autre catégorie de destinataires de données. Détaillez.

3. Données transférées

A. Quel est le nombre de personnes fichées concernées par le transfert?

B. Quel est le nombre de renseignements transférés?

C. Quel est le contenu des données transférées?

1. Données d'identification (nom, adresse, tél., n° de carte d'identité, de permis de conduire,...). Détaillez.

2. Caractéristiques personnelles (âge, sexe, état-civil, données physiques, nationalité, statut d'immigration, situation militaire, composition du ménage, loisirs et intérêts, habitudes de consommation, éducation et formation,...). Détaillez.

3. Données financières (identifiants financiers, revenus, possessions, investissements, crédits, emprunts, solvabilité, transactions financières, détails, relatifs à la pension ou aux assurances,...). Détaillez.

4. Données relatives à la profession et l'emploi (emploi actuel, détails sur la terminaison d'emploi, historique de carrière, historique de présence et disciplinaire, salaire, évaluation,...). Détaillez.

5. Données judiciaires (suspicions ou mises en accusation, condamnations et peines, mesures judiciaires,...). Détaillez.

6. Données médicales (Relatives à l'état de santé physique ou psychique, aux situations et comportements à risques, aux antécédents médicaux de la personnefichée,...). Détaillez.

7. Données relatives au comportement sexuel de la personne fichée. Détaillez.

8. Données relatives à l'origine raciale ou ethnique de la personne fichée. Détaillez.

9. Données relatives aux convictions religieuses, philosophiques ou politiques de la personne fichée. Détaillez.

10. Données relatives à l'affiliation syndicale de la personne fichée. Détaillez.

11. Autres catégories de données. Détaillez.

4. Finalité du traitement dans le pays tiers

A. Quelle est la finalité du traitement envisagé dans le pays tiers?

1. Gestion des entreprises (administration du personnel, planification des activités, gestion de la clientèle, gestion du contentieux, relations publiques, renseignements technico-commerciaux,...). Détaillez.

2. Justice et police (sécurité publique, enregistrement des condamnations,...). Détaillez.

3. Secteurs bancaire, du crédit et des assurances (gestion des comptes, octroi et gestion des crédits, services liés aux cartes de crédit, services de courtage, vision globale d'un client, gestion des assurances,...). Détaillez.

4. Commerce (vente par correspondance, profilage de la clientèle, marketing direct,...). Détaillez.

5. Enseignement et culture (administration des élèves, gestion de bibliothèque,...). Détaillez.

6. Soins de santé (soins des patients, administration des hôpitaux, enregistrements de groupes à risques, enregistrement de donneurs,...)

7. Recherche scientifique (recherches épidémiologiques, recherches bio-médicales,...). Détaillez.

8. Autres buts (à définir par le maître du fichier)

B. La finalité du traitement dans le pays tiers est-elle identique à celle poursuivie par l'émetteur des données

5. Périodicité du flux

Quelle est la fréquence des transferts pour lesquels l'autorisation est demandée?

- Permanent
- Régulier
- Exceptionnel

6. Durée de traitement prévue par le destinataire

A. Quelle durée de conservation est-elle envisagée pour les données après leur enregistrement par le destinataire?

1. Pas de conservation (destruction immédiate)`

2. Durée de conservation limitée (préciser dans ce cas la durée de conservation en mois et en années, et le but de la conservation- par exemple, à fin de preuve)

3. Durée de conservation illimitée (Préciser les raisons)

7. Moyens de transfert

A. Quel est le moyen de transfert choisi (réseau, transfert physique,...)?

B. S'il s'agit d'un réseau, s'agit-il d'un réseau fermé (ex: Galileo) ou ouvert (Internet)? Détailler.

II. Niveau de protection du pays tiers

1. Les principes de fond

Les questions qui suivent visent à déterminer si, dans l'un ou l'autre des moyens d'expression mentionnés par après (normes issues de l'autorité publique, standards, privacy policy, etc,...), les principes suivants sont exprimés, et selon quelles modalités.

8. Principe de participation individuelle

Le(s) moyen(s) d'expression existant(s) envisagent-ils les points suivants:

A. Les personnes concernées ont-elles la possibilité d'obtenir les informations qu'elles souhaitent sur le traitement des données les concernant?

B. Peuvent-elles prendre connaissance des données détenues par le responsable du traitement?

C. Peuvent-elles faire rectifier ou effacer les données incomplètes ou inexactes?

D. Le responsable du traitement a-t-il l'obligation de prendre l'initiative d'informer les personnes concernées sur le traitement qu'il effectue?

E. Le traitement peut-il se faire sans le consentement de la personne concernée?

F. Les personnes concernées ont-elles la possibilité de s'opposer au traitement des données les concernant? Pour quel motif? Cette possibilité existe-t-elle dans tous les secteurs?

9. Principe de finalité

A. Les moyens d'expression prévoient-ils que la ou les finalités du traitement des données collectées doivent être légitimes?

B. Quels critères permettent d'apprécier la légitimité?

C. Existe-il une liste des traitements toujours considérés comme illégitimes?

D. Cette exigence de légitimité peut-elle être supprimée (dans le cas où la personne concernée a donné son consentement au traitement de ses données, par exemple? Détaillez)

E. Les normes prévoient-elles des limites à la réutilisation des données?

F. Plus spécifiquement, prévoient-elles que les données peuvent être communiquées à un tiers ou utilisées à des fins autres que celles pour lesquelles elles ont été transférées par l'émetteur:

1. en aucun cas?

2. dans des cas précis (consentement de la personne, protection d'un intérêt public du pays tiers,...)? Détaillez.

G. Si ces réutilisations sont permises, existe-t-il des dispositions telles que:

1. l''information de la personne concernée. Par quel moyen? Quel est le contenu de cette information?

2. La possibilité pour la personne fichée de s'opposer à cette réutilisation?

3. Autres? Détaillez.

H. Les moyens d'expression prévoient-ils que la ou les finalités du traitement des données collectées doivent être déterminées (à quel moment doivent-elles être déterminées?)

I. Existe-t-il des mesures spécifiques de protection concernant les transferts transfrontières de données au départ du pays tiers? Lesquelles?

10. Principe de proportionnalité

A. Les données traitées doivent-elles être impérativement en rapport avec la finalité du traitement?

B. Ce rapport est-il défini strictement?

C. Des données peuvent-elles être conservées au-delà de la durée nécessaire à la réalisation du traitement correspondant à la finalité initiale?

11. Principe de qualité des données

A. Le(s) moyen(s) d'expression prévoient-ils des conditions de qualité des données?

B. Plus spécifiquement, est-il prévu que les données doivent être:

1. Tenues à jour? (Des mécanisme-s précis sont-ils exigés pour assurer la mise à jour?)

2. Exactes?

3. Complètes?

4. Autres exigences? Détaillez.

C. L'obligation mise à charge de l'utilisateur des données en matière de qualité des données est-elle une obligation de moyens ou de résultat?

2. Effectivité des principes de fond

2.A. Moyens d'expression et de sanction

Quelle est la nature des moyens d'expression des principes de fond dans le pays destinataire? (Répondez le cas échéant de manière distincte pour chaque principe)

12. Privacy Policy

A. L'entreprise destinataire a-t-elle une privacy policy?

B. Si oui, ce texte fait-il l'objet de publication ?

C. Ces publications sont-elles accessibles au public en général? Comment?

D. Quels sont les moyens internes mis en place au sein de l'entreprise destinataire pour contrôler le respect de la *privacy policy* ?

E. L'adoption d'une *privacy policy* est-elle une condition d'obtention d'un certificat ? du respect d'un code de conduite ?

F. Existe-t-il des recours mis en place par l'entreprise dans le cadre de la *privacy policy*?

- Quelles en sont les modalités? En particulier,

  La saisine est-elle aisée et gratuite?

  Les délais entre la saisine et le prononcé sont-ils fixés?

- Quel est l'objet de ce recours (obtention de dommages et intérêts, modification d'un comportement de l'entreprise, rectification ou effacement de données,...?)

G. A votre connaissance un tribunal peut-il sur base de sa *privacy policy* condamner l'entreprise destinataire en cas de non respect ?

13. Standardisation

A. L'entreprise ou organisme destinataire des données a-t-il obtenu un certificat de respect d'une norme fixée par un organisme de normalisation? Si oui, quel est cet organisme?

B. Cette norme implique-t-elle le respect de principes de fond de la protection des données? Enoncez le contenu des mesures concernant la protection de la vie privée.

C. Y a-t-il eu une participation à la conception du standard des différents acteurs intéressés à la protection des données? Par quel moyen?

D. Le standard en question, ainsi que ses conditions d'obtention, sont-ils publiés?

E. L'organisme certificateur ou d'autres sociétés effectuent-ils des missions d'audit afin de vérifier le respect de la norme? Si oui:

- quelles sont les conditions d'agréation de la société auditrice?

- à quelle fréquence l'audit se fait-il?

- quels sont les pouvoirs de sanction éventuels de la société auditrice?

F. Existe-t-il des possibilités de recours ouvertes aux particuliers auprès de l'organisme certificateur sur base de la norme?

- Ces possibilités de recours sont-elles rendues publiques?

- Sont-elles aisées (accessibilité, coût,...)?

G. Peut-on invoquer devant les tribunaux le contenu de la norme? Son non respect peut-il être considéré comme une violation des règles de l'art?

14. Code de conduite sectoriel

A. L'entreprise ou organisme destinataire des données respectent-ils un code de conduite contenant des dispositions en matière de principes de fond de la protection des données?

B. Ce code a-t-il été négocié avec des instances extérieures au secteur professionnel concerné? En particulier, les personnes concernées autres que les responsables du traitement ont-elles pu participer à sa conception?

C. De quelle représentativité au sein du secteur jouissent les associations qui ont promulgué ce code?

D. Ce code a-t-il été publié ou mis à disposition du public d'une autre façon?

E. Existe-t-il un mécanisme de contrôle du respect de ce code? Le code prévoit-il lui-même ce mécanisme, ou renvoie-t-il à un contrôle externe?

F. Le code prévoit-il des sanctions pour le non-respect des règles qu'il édicte? (exclusions de l'association sectorielle, sanctions financières, ...) Si non, renvoie-t-il à des sanctions externes?

G. Existe-t-il des possibilités de recours offertes aux particuliers en cas de non respect du code de conduite? Auprès de quelles instances (autorités sectorielles, tribunaux, autorité indépendante de contrôle?)

- La saisine est-elle aisée (accessibilité, coût...)?

- Les délais entre la saisine et le prononcé sont-ils raisonnables?

- Le prononcé est-il public?

H. Existe-t-il des sanctions en cas de non respect du code de conduite?

- De quelle instance émanent-elles?

- Quelle est la nature de ces sanctions?

15. Normes issues de l'autorité publique

A. Existe-t-il dans le pays (ou Etat, ou région) destinataire des normes issues de l'autorité publique ayant pour objet, direct ou indirect la protection des principes fondamentaux de protection des données? Dans l'affirmative, fournissez-en le texte.

B. La norme étend-elle la protection qu'elle institue aux étrangers non-résidents dans le pays tiers?

C. Quelle est la place, dans la hiérarchie du pays tiers, de l'autorité qui a édicté la norme?

D. S'agit-il d'une norme générale, sectorielle, ou spécifique à certaines activités ou opérations?

E. La norme prévoit-elle des sanctions?

- Si oui, de quelle nature sont-elles? (civiles, pénales,...)

- De quelle instance émanent-elles?

- Existe-t-il à votre connaissance, une jurisprudence en cette matière?

F. Existe-t-il des procédures particulières, accélérées ou simplifiées, d'introduction d'un recours fondé sur cette norme?

G. L'action d'intérêt collectif est-elle possible dans le système juridique dans lequel se situe la norme?

2.B. Moyens de contrôle

16. Mesures de sécurité

A. Existe-t-il dans l'entreprise ou organisme destinataire des données:

- des protections logiques, contrôlant les accès au réseau et aux fichiers? Lesquelles?

Les données transférées sont-elles cryptées? Si oui, quel est le système utilisé?

- des systèmes de sécurité physique protégeant les sites d'exploitation? Lesquels?

- des dispositifs de back-up, concernant aussi bien les réseaux que les fichiers (permettant de redémarrer rapidement après un incident)? Détailler.

- des mesures organisationnelles ayant pour objet d'assurer la sécurité interne des données?

B. Des mesures de sécurité sont-elles spécifiquement imposées par un des moyens d'expression cités ci-dessus (certification, code de conduite, norme issue de l'autorité publique,...)?

17. Autorité indépendante de contrôle

A. Existe-t-il une instance de contrôle du respect des principes de fond cités ci-dessus?

B. Est-ce une instance spécifique à la protection des données?

C. Par qui a-t-elle été instituée?

D. Quelle est sa composition?

- A-t-elle un personnel spécifique?

- A-t-elle un personnel permanent?

- Travaille-t-elle en relation avec des "relais" (organes de certification,...) dans certains secteurs?

E. Quels sont les missions et les compétences de cette instance?

F. Des mesures de publicité sont-elles prévues pour les décisions prises par cette instance? Lesquelles? Publie-t-elle un rapport d'activité?

G. A-t-elle des pouvoirs d'investigation:

- propres?

- avec le concours de l'autorité publique?

H. Les particuliers peuvent-ils introduire une plainte à propos d'un traitement de données les concernant auprès de cette instance?Si oui, selon quelles modalités (coût, délais,...)?

I. Cette instance dispose-t-elle de moyens de contrainte suffisants pour contraindre les responsables de traitements à suivre ses avis ou recommandations?

J. A-t-elle des pouvoirs de sanction propres?

- Si oui, lesquels,

- Le pouvoir judiciaire a-t-il l'obligation de sanctionner les infractions constatées par cette instance?

18. Accès des personnes concernées

A. Les personnes concernées reçoivent-elles une information au sujet du traitement opéré dans le pays tiers?

- A quel moment?

- L'information est-elle donnée spontanément par le maître du fichier, ou sur demande?

- Sur quels éléments porte l'information?

- Que peut exiger la personne concernée sur base de cette information (rectification, opposition au traitement, effacement des données,...)?

B. La personne concernée bénéficie-t-elle d'une aide pour lui faciliter l'accès à ses données (intervention d'une autorité indépendante de contrôle, d'un représentant en Europe, d'un détaché à la protection des données,...)?

C. L'exercice de l'accès est-il payant?

19. Détaché à la protection des données

A. Existe-t-il au sein de l'entreprise ou organisme destinataire des données une personne ou un service compétent pour vérifier à l'intérieur de l'organisation le respect des principes de protection des données et pour accueillir les plaintes et demandes des personnes concernées?

B. Le détaché a-t-il fait l'objet d'une désignation publique?

C. Quelle place occupe-t-il dans l'organigramme de l'entreprise ou organisme destinataire?

D. Le détaché rend-il public un rapport de ses missions?

E. Le détaché dispose-t-il de pouvoirs d'invetigation au sein de l'entreprise?

20. Représentant

A. L'entreprise a-t-elle chargé une organisation située sur le territoire de l'Union Européenne de veiller au respect des prescrits de la directive européenne à propos du traitement opéré dans le pays tiers?

B. La nomination du représentant a-t-elle été portée à la connaissance des personnes concernées? Par quel moyen?

C. Les missions du représentant sont-elles définies par un contrat?

- Quelles sont-elles?

- Le contenu de ce contrat est-il accessible aux personnes concernées ou aux autorités de protection des données?

D. Des sanctions sont-elles prévues pour le cas où le responsable du traitement à l'étranger ne respecte pas ses engagements (prévus éventuellement par le contrat)?

21. Audits

A. L'entreprise ou organisation destinataire des données est-elle soumise à un audit visant à vérifier le respect par elle:

- de mesures de sécurité?

- de l'ensemble des principes de fond de la protection des données?

B. Par qui cet audit est-il effectué?

C. La firme auditrice doit-elle:

- être agréée?

- répondre à des conditions d'indépendance par rapport à l'entreprise ou organisation faisant l'objet de l'audit?

D. Que comporte le mandat de l'auditeur en terme de pouvoirs d'investigation?

E. L'entreprise ou organisation faisant l'objet de l'audit est-elle tenue de suivre les recommandations de l'auditeur?

F. Les résultats de l'audit sont-ils rendus publics?

22. Moyens de contrôle préventifs à disposition d'autorités sectorielles ou de protection des données

A. Des mesures préventives telles que la mise à disposition d'information, ou des contrôles a priori des traitements, pèsent-elles sur l'entreprise destinataire des données? Détaillez ces mesures

B. Sont-elles rendues légalement obligatoire par une norme? Laquelle

C. Auprès de quel type d'organe (autorités sectorielles ou de protection des données) sont-elles organisées?.

D. Quel type de réaction les organes peuvent-ils avoir suite à ces mesures préventives (contrôle des traitements, injonctions vis-à-vis des responsables de traitement,...)

D. Ces autorités bénéficient-elles de moyens matériels (budget, personnel,...) pour mener à bien ces missions préventives?

- Leurs compétences sont-elles officiellement reconnues?

- Ces autorités bénéficient-elles d'un pouvoir d'investigation et de contrainte suffisant?